

Universidade Estadual de Campinas

Instituto de Matemática, Estatística  
e Computação Científica  
DEPARTAMENTO DE MATEMÁTICA

# Códigos Geométricos de Goppa Via Métodos Elementares

**Autor: Nolmar Melo de Souza**

**Orientador: Prof. Dr. Paulo Roberto Brumatti**

**Co-orientador: Prof. Dr. Fernando Eduardo  
Torres Orihuela**

## Códigos Geométricos de Goppa Via Métodos Elementares

Este exemplar corresponde à redação final da dissertação devidamente corrigida e defendida por Nolmar Melo de Souza e aprovada pela comissão julgadora.

Campinas, 16 de março de 2006



Prof. Dr. Paulo Roberto Brumatti

Orientador



Prof. dr. Fernando Eduardo Torres Orihuela

Co-orientador

Banca Examinadora:

1. Prof. Dr. Paulo Roberto Brumatti
2. Prof. Dr. Ercilio Carvalho da Silva
3. Prof. Dr. Reginaldo Palazzo Junior

**Dissertação de Mestrado** apresentada ao Instituto de Matemática, Estatística e Computação Científica como parte dos requisitos para obtenção do título de **Mestre em Matemática**. Área de concentração: **Álgebra**.

**FICHA CATALOGRÁFICA ELABORADA PELA  
BIBLIOTECA DO IMECC DA UNICAMP**

**Bibliotecária: Maria Júlia Milani Rodrigues - CRB8a /2116**

Melo, Nolmar

M491c      Códigos geométricos de Goppa via métodos elementares / Nolmar Melo de Souza – Campinas, [S.P.:s.n.], 2006.

Orientadores: Paulo Roberto Brumatti; Fernando Eduardo Torres Orihuela  
Dissertação (mestrado) - Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Códigos de controle de erros (Teoria da informação). 2. Semigrupos. 3. Geometria algébrica. 4. Teoria da codificação. I. Brumatti, Paulo Roberto. II. Torres Orihuela, Fernando Eduardo. III. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. IV. Título

Título em inglês: Goppa geometry codes via elementary methods

Palavras-chave em inglês (Keywords): 1. Error control codes (Information theory). 2. Semigroups. 3. Algebraic geometry. 4. Coding theory.

Área de concentração: Álgebra

Titulação: Mestre em Matemática

Banca examinadora: Prof. Dr. Paulo Roberto Brumatti (IMECC-UNICAMP)  
Prof. Dr. Ercílio Carvalho da Silva (UFU-MG)  
Prof. Dr. Reginaldo Palazzo Junior (FEEC-UNICAMP)

Data da defesa: 17/02/2006

Dissertação de Mestrado defendida em 17 de fevereiro de 2006 e aprovada

Pela Banca Examinadora composta pelos Profs. Drs.



---

Prof. (a). Dr (a). PAULO ROBERTO BRUMATTI



---

Prof. (a). Dr (a). ERCILIO CARVALHO DA SILVA



---

Prof. (a). Dr (a). REGINALDO PALAZZO JUNIOR

# Resumo

O objetivo central desta dissertação foi o de apresentar os Códigos Geométricos de Goppa via métodos elementares que foram introduzidos por J. H. van Lint, R. Pellikaan e T. Høhold por volta de 1998. Numa primeira parte da dissertação são apresentados os conceitos fundamentais sobre corpos de funções racionais de uma curva algébrica na direção de se definir os códigos de Goppa de maneira clássica, neste estudo nos baseamos principalmente no livro “Algebraic Function Fields and Codes” de H. Stichtenoth. A segunda parte inicia-se com a introdução dos conceitos de funções peso, grau e ordem que são fundamentais para o estudo dos Códigos de Goppa via métodos elementares de álgebra linear e de semigrupos, tal estudo foi baseado em “Algebraic geometry codes” de J. H. van Lint, R. Pellikaan e T. Høhold.

A dissertação termina com a apresentação de exemplos que ilustram os métodos elementares que nos referimos acima.

# Abstract

The central objective of this dissertation was to present the Goppa Geometry Codes via elementary methods which were introduced by J.H. van Lint, R.Pellikaan and T. Høhold about 1998. On the first part of such dissertation are presented the fundamental concepts about fields of rational functions of an algebraic curve in the direction as to define the Goppa Codes on a classical manner. In this study we based ourselves mainly on the book “Algebraic Function Fields and Codes” of H. Stichtenoth. The second part is initiated with an introduction about the functions weight, degree and order which are fundamental for the study of the Goppa Codes through elementary methods of linear algebra and of semigroups and such study was based on “Algebraic Geometry Codes” of J.H. van Lint, R.Pellikaan and T. Høhold.

The dissertation ends up with a presentation of examples which illustrate the elementary methods that we have referred to above.

Dedico esse trabalho a aqueles que me apoiaram incondicionalmente, meus pais. João Ferreira de Souza e Maria de Fátima Mello de Souza.

# Agradecimentos

Agradeço:

Por sua grande atenção, paciência e dedicação agradeço em especial ao professor Paulo Roberto Brumatti, que me orientou na condução deste trabalho.

Ao professor Fernando Torres, o qual contribuiu com valiosas dicas de como prosseguir os estudos que levaram a construção deste.

Aos meus pais e irmãos que me apoiaram em todos os momentos da vida.

Ao professor Haroldo Benatti, que com sua dedicação me incentivou a continuar os estudos após a graduação.

À José Santana, que me apoiou em vários momentos.

Aos meus amigos, sem os quais seria difícil concluir essa etapa.

À Capes, pelo apoio financeiro.



lance de dados  
(gessinger)

daqui não tem mais volta, pra frente é sem saber  
pequenos paraísos e riscos a correr  
os deuses jogam pôquer  
e bebem no saloon doses generosas de br 101  
tá escrito há 6.000 anos em parachoques de caminhão  
atalhos perigosos feito frases feitas  
os deuses dão as cartas... o resto é com você

no fundo tudo é ritmo  
a dança foge do salão  
invade a autoestrada do átomo ao caminhão  
o fim é puro ritmo  
o último suspiro é purificação  
os deuses dão as costas... agora é só você  
  
os deuses dão as costas... agora é só você... querer

# Sumário

<b>Introdução</b>	<b>1</b>
<b>1 Noções Básicas</b>	<b>3</b>
1.1 Códigos . . . . .	3
1.2 Códigos Lineares . . . . .	4
1.3 Lugares . . . . .	7
1.4 O Corpo de Funções Racionais . . . . .	11
1.5 Divisores . . . . .	11
1.6 O Teorema de Riemann-Roch . . . . .	14
1.7 Curvas Algébricas . . . . .	17
1.7.1 Variedades Projetivas . . . . .	19
1.7.2 Curvas Não Singulares . . . . .	20
<b>2 Códigos Algébricos Geométricos</b>	<b>21</b>
2.1 Códigos Algébricos Geométricos . . . . .	21
2.2 Teorema de Bézout . . . . .	27
<b>3 Códigos de Avaliação</b>	<b>29</b>
3.1 Funções Peso, Grau e Ordem . . . . .	29
3.2 Códigos de Avaliação . . . . .	33
3.3 A Cota Ordem . . . . .	34
3.4 Semigrupos . . . . .	36
3.5 Código de Avaliação Via Semigrupos . . . . .	40

<b>4 Exemplos</b>	<b>42</b>
4.1 Um Primeiro Exemplo . . . . .	42
<b>Referências Bibliográficas</b>	<b>48</b>

# Introdução

A teoria de códigos corretores de erros teve início com as pesquisas de matemáticos da Bell Lab. na década de 1940. Apesar da grande utilização na engenharia, a teoria utiliza de sofisticadas técnicas matemáticas fazendo uso de várias áreas tais como Geometria Algébrica, Teoria dos Números, Teoria dos Grupos e Combinatória.

Os códigos corretores de erros estão presentes no nosso cotidiano sempre que usamos o computador (no uso da internet ou na armazenagem de dados, por exemplo), transmitimos dados, assistimos um DVD, etc.

Os códigos algébricos geométricos, que são uma sub-classe dos códigos lineares (subespaços linear de um determinado espaço vetorial munido com uma métrica), foram inicialmente apresentados por V. D. Goppa num artigo, [3], publicado em 1981. Essa classe de códigos, que é uma das mais estudadas atualmente, utiliza como ferramenta principal a geometria algébrica.

Nesse texto apresentamos os códigos de avaliação, que foram introduzidos por Tom Høholdt, Jacobus H. van Lint e Ruud Pellikaan através das funções ordem e peso. Tais códigos têm um tratamento muito mais simples do que os códigos algébricos, geométricos visto que estes usam como teorias base os semigrupos e a álgebra linear.

O primeiro capítulo desse texto, capítulo onde a maioria das proposições tiveram suas demonstrações omitidas, traz uma introdução à teoria de códigos e também algumas ferramentas da geometria algébrica tendo como um dos principais resultados o teorema de Riemann-Roch.

Já no segundo capítulo fazemos uma apresentação dos códigos algébricos geométricos, códigos que também são chamados de **códigos geométricos de**

**Goppa.** Tal apresentação é feita de maneira sucinta.

No terceiro capítulo trazemos as funções ordem, peso e grau, que são fundamentais para calcularmos os parâmetros dos códigos de avaliação, que ali também são apresentados. Tais funções, unidas à teoria de semigrupo, nos permite descrever os códigos de avaliação de modo simples, fazendo desses uma alternativa aos códigos algébricos geométricos.

No quarto e último capítulo fazemos a conexão entre códigos de Goppa pontuais e códigos de avaliação e apresentamos alguns exemplos. Ali tentamos mostrar de modo prático a diferença entre ambos os códigos e ao mesmo tempo a proximidade dos dois.

# Capítulo 1

## Noções Básicas

Este capítulo está dedicado a introdução da notação que utilizaremos, assim como expor definições e teoremas clássicos da teoria, os quais, na maioria das vezes, terão suas demonstrações omitidas, visto que a bibliografia indicada ao final desse texto as fazem muito bem. Um dos principais teoremas que iremos encontrar aqui é o Teorema de Riemann-Roch.

### 1.1 Códigos

Nessa seção iremos introduzir um dos principais objetos que serão tratados nesse texto (código). Usaremos aqui um conjunto  $Q$  com  $q$  elementos e o chamaremos de alfabeto.

**Definição 1.1.1.** *A um subconjunto próprio não vazio,  $C$ , de  $Q^n$ , damos o nome de código. Chamaremos de palavras código de comprimento  $n$  aos seus elementos.*

Dizemos que um código  $C$  é trivial se  $\#C = 1$ .

Em seguida apresentamos as definições elementares e o resultado, proposição 1.1.5, que caracteriza os códigos perfeitos.

**Definição 1.1.2** (Distância de Hamming). *Sendo  $x, y \in Q^n$  definimos distância de  $x$  à  $y$  como:*

$$d(x, y) = \#\{i; 1 \leq i \leq n \text{ e } x_i \neq y_i\}.$$

**Definição 1.1.3.** Quando  $Q$  é um corpo e  $x \in Q^n$  o peso de  $x$  é definido como  $w(x) = d(x, 0)$ .

**Definição 1.1.4.** Chamamos de distância mínima do código  $C$  ao natural  $d = \min\{d(x, y); x, y \in C\}$ .

**Proposição 1.1.5.** Dado um código com distância mínima  $d = 2e + 1$  temos que as bolas do conjunto  $B = \{B[x, e]; x \in C\}$  são disjuntas, onde  $B[x, e] = \{y \in Q^n; d(x, y) \leq e\}$ .

*Demonstração.* Segue diretamente da desigualdade triangular visto que a distância de Hamming é uma métrica.  $\square$

**Observação 1.1.6.** Dizemos que um código com distância mínima  $d = 2e + 1$  detecta  $2e$  e corrige  $e$  erros, ou seja, ocorrendo até  $e$  erros é possível decodificar a palavra código transmitida.

**Definição 1.1.7.** Um código  $C \subset Q^n$  com distância mínima  $2e + 1$  é dito código perfeito se  $Q^n = \dot{\bigcup}_{x \in C} B(x, e)$ .

## 1.2 Códigos Lineares

Nessa seção definiremos uma das principais classes de códigos e para tais códigos o alfabeto,  $Q$ , é um corpo finito  $\mathbb{F}_q$  com  $q$  elementos, onde  $q = p^r$  e  $p$  é um número primo.

**Definição 1.2.1** (Código Linear). Um código linear  $C$  sobre um alfabeto  $\mathbb{F}_q$  é um  $\mathbb{F}_q$ -subespaço vetorial de  $\mathbb{F}_q^n$ . Se  $\dim_{\mathbb{F}_q}(C) = k$  chamamos  $C$  de um  $[n, k]$ -código.

Usaremos a notação  $[n, k, d]$ -código, para um código linear com distância mínima  $d$ .

**Teorema 1.2.2.** Num código linear a distância mínima é igual ao peso mínimo.

*Demonstração.* Como  $C$  é um subespaço vetorial e dados  $x, y \in C$  temos que  $x - y \in C$ . Sejam  $x, y \in C$  tais que  $d(x, y)$  seja mínima. Logo  $d(x, y) = d(x - y, 0) = w(x - y)$  e mais  $w(x - y)$  é mínimo.  $\square$

Na descrição de um código linear um importante ingrediente é o que se chama **matriz geradora**.

**Definição 1.2.3.** *Uma matriz  $k \times n$ ,  $G$ , é dita geradora de um código linear  $C$  se os seus vetores linha formam uma base para  $C$ .*

**Definição 1.2.4.** *Dizemos que uma matriz geradora,  $G$ , de um código linear,  $C$ , está na forma padrão se esta matriz está escrita em blocos da seguinte maneira:*

$$G = [I_k | P]$$

onde  $I_k$  é a matriz identidade  $k \times k$  e  $P$  é uma  $k \times (n - k)$  matriz.

Em [4] vemos que nem todo código tem uma matriz geradora na forma padrão, contudo vê-se também que pode-se definir **códigos equivalentes** com os mesmos parâmetros  $n$ ,  $k$  e  $d$  de modo que essa possua uma matriz geradora na forma padrão.

**Proposição 1.2.5.** *O complemento ortogonal de um  $[n, k, d]$ -código  $C$ , em relação ao produto interno canônico<sup>1</sup>, também é um código e esse é chamado código dual e denotado por  $C^\perp$ . Além disso a dimensão do código dual é  $n - k$  e mais, sendo  $G = [I_k | P]$  a matriz geradora do código  $C$ , então  $H = [-P^t | I_{n-k}]$  é a matriz geradora do código dual  $C^\perp$ . A matriz  $H$  assim definida é dita matriz de teste de paridade pois  $x \in C$  se, e somente se,  $Hx^t = 0$ .*

A proposição acima nos dá uma informação muito importante sobre a pertinência de uma dada palavra ao código, o que é fundamental para a sua decodificação. Assim ficam justificadas a definição e o resultado que apresentaremos a seguir:

**Definição 1.2.6.** *Sendo  $C$  um código linear com matriz de teste de paridade  $H$ , então para todo  $x \in \mathbb{F}_q^n$  chamamos  $Hx^t$  de síndrome de  $x$ .*

**Teorema 1.2.7.** *Dados  $x, y \in \mathbb{F}_q^n$  então  $x$  e  $y$  tem a mesma síndrome se, e somente se,  $x - y \in C$ .*

---

<sup>1</sup>Dados dois vetores em  $\mathbb{F}_q^n$ ,  $a = (a_1, \dots, a_n)$  e  $b = (b_1, \dots, b_n)$ , definimos o produto interno canônico como  $\langle a, b \rangle = \sum_{i=1}^n a_i b_i$ .



*Demonstração.* Seja  $H$  a matriz de teste de paridade do código  $C$ , então temos:

$$Hx^t = Hy^t \Leftrightarrow Hx^t - Hy^t = 0 \Leftrightarrow H(x - y)^t = 0 \Leftrightarrow x - y \in C.$$

□

As definições e resultados que apresentaremos abaixo estão todos relacionados com a codificação de uma mensagem enviada.

**Definição 1.2.8.** *Seja  $c$  uma palavra transmitida e  $x$  o vetor recebido, definimos o vetor erro como sendo  $e = x - c$ , observamos que a quantidade de erros ocorridos na transmissão é o peso de  $e$ .*

**Definição 1.2.9.** *Dizemos que dois vetores estão numa mesma classe lateral se eles tem a mesma síndrome. Um vetor de menor peso na classe é dito líder.*

**Teorema 1.2.10.** *Sendo  $C$  um  $[n, k, d]$ -código, se  $u \in \mathbb{F}_q^n$  é tal que  $w(u) \leq \left\lfloor \frac{d-1}{2} \right\rfloor$  então  $u$  é o líder de sua classe.*

*Demonstração.* Sejam  $u, v \in \mathbb{F}_q^n$ , com  $w(u) \leq \left\lfloor \frac{d-1}{2} \right\rfloor$  e  $w(v) \leq \left\lfloor \frac{d-1}{2} \right\rfloor$ , se  $u - v \in C$  temos que  $w(u - v) \leq w(u) + w(v) \leq \left\lfloor \frac{d-1}{2} \right\rfloor + \left\lfloor \frac{d-1}{2} \right\rfloor \leq d - 1$ , logo  $u - v = 0$ , assim temos que  $u = v$ . □

**Teorema 1.2.11.** *Sendo  $H$  uma matriz de teste de paridade de  $C$  temos que  $w(C) \geq r$  se, e somente se, quaisquer  $r - 1$  colunas de  $H$  são linearmente independentes (L.I.).*

*Demonstração.*  $\Leftarrow$ ) Seja  $c \in C$ ,  $c \neq 0$ ,  $H = [h_1, h_2, \dots, h_n]$ . Então  $0 = Hc^t = \sum_{i=1}^n c_i h_i$ . Logo  $w(c) \geq r$ , pois, caso contrário teríamos uma combinação linear de  $r - 1$  vetores L.I. dando zero.

$\Rightarrow$ ) Suponha que exista  $r - 1$  colunas L.D., sem perda de generalidade podemos supor que são as  $r - 1$  primeiras colunas  $h_1, \dots, h_{r-1}$ . Logo existem  $c_1, \dots, c_{r-1} \in \mathbb{F}_q$ , não todos nulos, com  $\sum_{i=1}^{r-1} c_i h_i = 0$ . Assim  $c = (c_1, \dots, c_{r-1}, 0, \dots, 0) \in C$  pois  $Hc^t = 0$  e  $w(c) \leq r - 1$ , absurdo. □

Uma cota que relaciona os parâmetros de um código aparecem no teorema:

---

<sup>2</sup>A notação  $\left\lfloor \frac{a}{b} \right\rfloor$  denota o maior inteiro menor ou igual a  $\frac{a}{b}$ .

**Teorema 1.2.12** (Cota de Singleton). *Seja  $C$  um  $[n, k, d]$ -código linear, então  $d \leq n - k + 1$ . Chamamos de código MDS (Maximum Distance Separable) ao código tal que  $d = n - k + 1$ .*

*Demonstração.* Seja  $H$  a matriz de teste de paridade de  $C$ . Logo, posto de  $H = n - k$ . Do teorema 1.2.11 segue que quaisquer  $(d - 1)$  colunas de  $H$  são L.I.. Assim  $d - 1 \leq (\text{posto de } H)$ , temos que  $d \leq n - k + 1$ .  $\square$

## 1.3 Lugares

Nessa seção apresentaremos as estruturas necessárias para a definição dos códigos algébricos geométricos que veremos no próximo capítulo.

**Definição 1.3.1.** *Um corpo de funções algébricas  $F/K$  de uma variável sobre  $K$  é uma extensão de corpos  $F \supset K$  tal que  $F$  é uma extensão algébrica finita de  $K(x)$  com  $x \in F$  e transcendente sobre  $K$ .*

O conjunto  $\tilde{K} = \{a \in F; a \text{ é algébrico em } K\}$  é um subcorpo de  $F$  e mais  $F/\tilde{K}$  é um corpo de funções algébricas sobre  $\tilde{K}$ . Esse conjunto é chamado de **corpo de constantes** de  $F/K$ . Neste trabalho vamos supor sempre que  $K = \tilde{K}$ .

**Exemplo 1.3.2** (Corpo de Funções racionais). O corpo de funções  $F/K$  é dito racional se  $F = K(x)$  para algum  $x$  que é transcendente sobre  $K$ , onde  $K(x)$  é o corpo de frações do anel de polinômios,  $K[x]$ , em uma variável sobre o corpo  $K$ .

Qualquer elemento não nulo,  $z \in K(x)$ , tem uma única representação

$$z = a \prod_i P_i(x)^{n_i}$$

com  $0 \neq a \in K$ ,  $P_i(x) \in K[x]$  mônicos irredutíveis distintos e  $n_i \in \mathbb{Z}$ .

A próxima definição nos traz um tipo de anel fundamental para o desenvolvimento do nosso trabalho.

**Definição 1.3.3.** *Um anel de valorização de um corpo de funções  $F/K$  é um sub-anel  $\mathcal{O} \subset F$  com as seguintes propriedades:*

1.  $K \subsetneq \mathcal{O} \subsetneq F$ ;

2. Para qualquer  $z \in F$ ,  $z \in \mathcal{O}$  ou  $z^{-1} \in \mathcal{O}$ .

**Exemplo 1.3.4.** No corpo de funções racionais  $K(x)$  aparecem os primeiros anéis de valorizações fundamentais, a saber:

Seja  $p(x) \in K[x]$ , um polinômio irredutível. Definimos o conjunto

$$\mathcal{O}_{p(x)} = \left\{ \frac{f(x)}{g(x)}; f(x), g(x) \in K[x], p(x) \nmid g(x) \right\}.$$

Assim definido,  $\mathcal{O}_{p(x)}$  é um anel de valorização de  $K(x)/K$ . Observe que se  $q(x)$  for outro polinômio irredutível, não associado a  $p(x)$ , temos que  $\mathcal{O}_{p(x)} \neq \mathcal{O}_{q(x)}$ .

Os anéis de valorizações são caracterizados, segundo sua estrutura, pelos resultados:

**Proposição 1.3.5.** *Seja  $\mathcal{O}$  um anel de valorização do corpo de funções  $F/K$  então:*

- a.  $\mathcal{O}$  é anel local, isto é  $\mathcal{O}$  tem um único ideal maximal  $P = \mathcal{O} \setminus \mathcal{O}^*$ , onde  $\mathcal{O}^*$  é o conjunto das unidades de  $\mathcal{O}$ ;
- b. Para  $0 \neq x \in F$ ,  $x \in P \Leftrightarrow x^{-1} \notin \mathcal{O}$ ;
- c. Para o corpo de constantes  $\tilde{K}$  de  $F/K$  temos que  $\tilde{K} \subset \mathcal{O}$  e  $\tilde{K} \cap P = 0$ .

Do item (b), segue que  $\mathcal{O}$  é unicamente determinado por  $P$ . De fato,  $\mathcal{O}_P := \mathcal{O} = \{x \in F; x \notin P\}$ .

**Teorema 1.3.6.** *Seja  $\mathcal{O}$  um anel de valorização do corpo de funções  $F/K$  e  $P$  o seu ideal maximal. Então,*

- a.  $P$  é principal;
- b. Se  $P = t\mathcal{O}$  então qualquer  $0 \neq z \in F$  tem uma única representação da forma  $z = t^n u$ , para algum  $n \in \mathbb{Z}$  e  $u \in \mathcal{O}^*$ ;
- c.  $\mathcal{O}$  é um domínio principal.

Os anéis de valorização nos levam a um outro conceito, a saber, o conceito de lugar.

**Definição 1.3.7.** 1. Um lugar  $P$  do corpo de funções  $F/K$  é um ideal maximal de algum anel de valorização de  $F/K$ . Qualquer elemento  $t$  que gera  $P$  ( $P = t\mathcal{O}$ ) é dito elemento principal de  $P$ ;

2.  $\mathbb{P}_F = \{P; P \text{ é lugar em } F/K\}$ .

Também um lugar dá origem a uma função especial que definiremos a seguir:

**Definição 1.3.8.** Uma valorização discreta de  $F/K$  é uma função  $v : F \rightarrow \mathbb{Z} \cup \{\infty\}$  com as seguintes propriedades:

1.  $v(x) = \infty \Leftrightarrow x = 0$ ;
2.  $v(xy) = v(x) + v(y)$ , para qualquer  $x, y \in F$ ;
3.  $v(x + y) \geq \min\{v(x), v(y)\}$ , para qualquer  $x, y \in F$ ;
4. Existe  $z \in F$  com  $v(z) = 1$ ;
5.  $v(a) = 0$ , para todo  $a \in K$ .

**Definição 1.3.9.** Para  $P \in \mathbb{P}_F$  associamos uma função de valorização,  $v_P : F \rightarrow \mathbb{Z} \cup \{\infty\}$ , da seguinte maneira: dado um elemento principal  $t \in P$  temos que todo elemento  $0 \neq z$  em  $F$  é escrito de maneira única na forma  $z = t^n u$ , com  $n \in \mathbb{Z}$  e  $u \in \mathcal{O}_P^*$ . Assim fazemos  $v_P(z) = n$  e  $v_P(0) = \infty$ .

Um primeiro resultado importante a respeito de  $v_P$  é dado no seguinte teorema:

**Teorema 1.3.10.** Seja  $F/K$  um corpo de funções então:

- a. Para qualquer  $P \in \mathbb{P}_F$ , a função de valorização  $v_P$  definida como acima é uma valorização discreta que satisfaz:
  - a.1.  $\mathcal{O}_P = \{z \in F; v_P(z) \geq 0\}$ ;
  - a.2.  $\mathcal{O}_P^* = \{z \in F; v_P(z) = 0\}$ ;
  - a.3.  $P = \{z \in F; v_P(z) > 0\}$ ;
  - a.4. Um elemento  $x \in F$  é principal de  $P$  se, e somente se,  $v_P(x) = 1$ .

b. Qualquer anel de valorização  $\mathcal{O}$  de  $F/K$  é um subanel maximal de  $F$ .

Definiremos agora alguns elementos da teoria que serão muito utilizados em nossa explanação.

**Definição 1.3.11.** *Sejam  $P \in \mathbb{P}_F$  e  $F_P = \mathcal{O}_P/P$  o corpo de resíduos de  $P$ . A aplicação  $x \mapsto x(P)$  de  $F$  em  $F_P \cup \{\infty\}$ , onde  $x(P) = x + P$  se  $x \in \mathcal{O}_P$  e  $x(P) = \infty$  se  $x \notin \mathcal{O}_P$ , é chamada de aplicação de resíduos com respeito a  $P$ .*

Pode-se provar que (veja em [7]) se  $P \in \mathbb{P}_F$  então  $K \subset F_P$  e  $F_P/K$  é uma extensão finita e assim definimos:

**Definição 1.3.12.** *Se  $P \in \mathbb{P}_F$  definimos o grau de  $P$  como sendo:*

$$gr(P) = [F_P : K].$$

Os conceitos de zeros e pólos são de importância fundamental para a descrição dos códigos algébricos geométricos.

**Definição 1.3.13.** *Seja  $z \in F$  e  $P \in \mathbb{P}_F$ . Dizemos que  $P$  é um zero de  $z$  se, e somente se,  $v_P(z) > 0$ , e  $P$  é um pólo de  $z$  se, e somente se,  $v_P(z) < 0$ . Se  $v_P(z) = m > 0$  falamos que  $P$  é um zero de ordem  $m$  e se  $v_P(z) = -m < 0$  dizemos que é um pólo de ordem  $m$ .*

O próximo resultado, chamado de teorema da aproximação fraca, vai ser útil na descrição de um dos códigos que iremos definir.

**Teorema 1.3.14** (Aproximação Fraca). *Sejam  $F/K$  um corpo de funções,  $P_1, \dots, P_n \in \mathbb{P}_F$  lugares de  $F/K$ , dois a dois distintos,  $x_1, \dots, x_n \in F$  e  $r_1, \dots, r_n \in \mathbb{Z}$ . Então, existe  $x \in F$  tal que:*

$$v_{P_i}(x - x_i) = r_i, \text{ para } i = 1, \dots, n.$$

**Corolário 1.3.15.** *O corpo de funções possui infinitos lugares.*

## 1.4 O Corpo de Funções Racionais

Como definimos anteriormente, o corpo de funções racionais é o próprio corpo de frações  $K(x)/K$ . Já tínhamos definido o anel de valorização

$$\mathcal{O}_{p(x)} = \left\{ \frac{f(x)}{g(x)}; f(x), g(x) \in K[x], p(x) \nmid g(x) \right\},$$

para um polinômio  $p(x) \in K[x]$  irredutível. Observamos agora que para esse anel, o ideal

$$P_{p(x)} = \left\{ \frac{f(x)}{g(x)}; f(x), g(x) \in K[x], p(x) \mid f(x), p(x) \nmid g(x) \right\},$$

é seu único ideal maximal. Consideremos agora um outro anel de valorização

$$\mathcal{O}_\infty = \left\{ \frac{f(x)}{g(x)}; f(x), g(x) \in K[x], \text{gr}(f(x)) \leq \text{gr}(g(x)) \right\},$$

que tem como ideal maximal

$$P_\infty = \left\{ \frac{f(x)}{g(x)}; f(x), g(x) \in K[x], \text{gr}(f(x)) < \text{gr}(g(x)) \right\}.$$

Na realidade estes são os únicos anéis de valorizações de  $K(x)$  e tal fato é expresso no resultado:

**Teorema 1.4.1.** *Os únicos lugares de  $K(x)/K$  são os da forma  $P_{p(x)}$  e  $P_\infty$  como acima definidos.*

## 1.5 Divisores

Nessa seção estaremos preocupados com a definição dos divisores de um corpo de funções, os quais serão fundamentais para a construção de alguns dos códigos que trataremos neste trabalho.

**Definição 1.5.1.** *O grupo aditivo abeliano livre que tem como base livre os lugares de  $F/K$  é denotado por  $\mathcal{D}_F$  e é chamado de grupo de divisores de  $F/K$ . Os elementos de  $\mathcal{D}_F$  são chamados de divisores e são da forma*

$$D = \sum_{P \in \mathbb{P}_F} n_P P, \text{ com } n_P \in \mathbb{Z}, \text{ único e quase sempre nulo.}$$

Chamamos de **suporte de um divisor**  $D$  o conjunto dos lugares  $P$  tais que  $n_P \neq 0$  e denotamos por  $\text{supp}(D)$ . Dados dois divisores  $D = \sum n_P P$  e  $D' = \sum n'_P P$  a soma deles é dada por:

$$D + D' = \sum_{P \in \mathbb{P}_F} (n_P + n'_P) P.$$

E mais, para cada  $P \in \mathbb{P}_F$ , definimos  $v_P(D) = n_P$ , assim também podemos definir uma ordem parcial de  $\mathcal{D}_F$  por

$$D_1 \leq D_2 \Leftrightarrow v_P(D_1) \leq v_P(D_2), \forall P \in \mathbb{P}_F.$$

Chamamos de grau de um divisor  $D$  ao número  $gr(D) = \sum_{P \in \mathbb{P}_F} v_P(D) gr(P)$ .

Definiremos agora os divisores principais, os quais trazem importantes conseqüências para a teoria. Pode-se provar, veja em [7], que se  $x \in F$  então o número de zeros e pólos de  $x$  é finito e esse fato nos leva a seguinte definição:

**Definição 1.5.2.** *Seja  $0 \neq x \in F$  e denotemos por  $Z$  e  $N$  o conjunto de zeros e pólos de  $x$  em  $\mathbb{P}_F$ , respectivamente, assim definimos:*

1.  $(x)_0 = \sum_{P \in Z} v_P(x) P$ , o divisor de zeros de  $x$ ;
2.  $(x)_\infty = \sum_{P \in N} (-v_P(x)) P$ , o divisor de pólos de  $x$ ;
3.  $(x) = (x)_0 - (x)_\infty$ , o divisor principal de  $x$ .

**Definição 1.5.3.** *Definimos o **grupo de divisores principais** de  $F/K$  como sendo  $\mathcal{P}_F = \{(x); 0 \neq x \in F\}$  (este é um subgrupo de  $\mathcal{D}_F$  desde que para  $0 \neq x, y \in F$ ,  $(xy) = (x) + (y)$ ). O quociente  $\mathcal{C}_F = \mathcal{D}_F / \mathcal{P}_F$  é chamado grupo de classe de divisores e dizemos que  $D$  é equivalente a  $D'$ , denotando por  $D \sim D'$ , se  $[D] = [D']$ , isto é, se  $D' = (x) + D$  para algum  $x \in F$ .*

Agora vamos definir um espaço vetorial associado a um divisor, o qual nos dará a definição de dimensão desse divisor e também de um invariante muito importante para a teoria.

**Definição 1.5.4.** *Para um divisor  $A \in \mathcal{D}_F$  definimos o conjunto*

$$\mathcal{L}(A) = \{x \in F; (x) \geq -A\} \cup \{0\}.$$

**Lema 1.5.5.** *Seja  $A \in \mathcal{D}_F$  então temos*

- a.  $\mathcal{L}(A)$  é um  $K$ -espaço vetorial, de dimensão finita;*
- b. Se  $A' \sim A$  então  $\mathcal{L}(A') \simeq \mathcal{L}(A)$ .*

**Definição 1.5.6.** *Para  $A \in \mathcal{D}_F$ , definimos a dimensão do divisor  $A$  como sendo  $\dim(A) = \dim_K(\mathcal{L}(A))$ .*

**Teorema 1.5.7.** *Qualquer divisor principal tem grau zero. Mais precisamente dado  $x \in F \setminus K$  e  $(x)_0, (x)_\infty$  denotando os divisores de zeros e pólos, respectivamente, do divisor de  $x$ , então:*

$$gr((x)_0) = gr((x)_\infty) = [F : K(x)].$$

Como consequência imediata deste teorema temos:

**Corolário 1.5.8.** *1. Seja  $A, A'$  divisores tais que  $A \sim A'$ . Assim temos que  $\dim(A) = \dim(A')$  e que  $gr(A) = gr(A')$ ;*

*2. Se  $gr(A) < 0$  então  $\dim(A) = 0$ ;*

*3. Para um divisor  $A$  de grau zero, temos que são equivalentes:*

- (a)  $A$  é um divisor principal;*
- (b)  $\dim(A) > 0$ ;*
- (c)  $\dim(A) = 1$ .*

A partir da proposição que enuciaremos a seguir definimos o gênero de um corpo de funções algébricas que é um invariante que depende apenas do corpo.

**Proposição 1.5.9.** *Existe uma constante  $\gamma \in \mathbb{Z}$  tal que, para todo divisor  $A \in \mathcal{D}_F$  temos que:*

$$gr(A) - \dim(A) \leq \gamma.$$

**Definição 1.5.10.** *Definimos o gênero do corpo de funções  $F/K$  como sendo*

$$g = \max\{gr(A) - \dim(A) + 1; A \in \mathcal{D}_F\}.$$



O primeiro resultado envolvendo o gênero de um corpo de funções é o seguinte:

**Teorema 1.5.11** (Teorema de Riemann). *Seja  $F/K$  uma corpo de funções algébricas com gênero  $g$  então:*

1. *Para qualquer divisor  $A \in \mathcal{D}_F$ ,  $\dim(A) \geq gr(A) + 1 - g$ ;*
2. *Existe um inteiro  $c$ , dependendo de  $F/K$  tal que  $\dim(A) = gr(A) + 1 - g$  sempre que  $gr(A) \geq c$ .*

## 1.6 O Teorema de Riemann-Roch

Aqui  $F/K$  denota um corpo de funções algébricas com gênero  $g$ .

**Definição 1.6.1.** *Para  $A \in \mathcal{D}_F$  definimos o índice de especialidade de  $A$  como sendo:*

$$i(A) = \dim(A) - gr(A) + g - 1.$$

Como se vê o Teorema de Riemann garante que o índice de especialidade de um divisor  $A$  é inteiro não negativo e na verdade nós vamos apresentar  $i(A)$  como a dimensão de certos espaços vetoriais. Assim para isto começamos com as definições abaixo:

**Definição 1.6.2.** *Um adele de  $F/K$  é uma função*

$$\begin{aligned} \alpha: \mathbb{P}_F &\rightarrow F \\ P &\mapsto \alpha_P \end{aligned}$$

*tal que  $\alpha_P \in \mathcal{O}_P$  para quase todos  $P \in \mathbb{P}_F$ . Podemos ver um adele como um elemento do produto direto  $\prod_{P \in \mathbb{P}_F} F$  e usamos a notação  $\alpha = (\alpha_P)_{P \in \mathbb{P}_F}$ , e para encurtar,  $\alpha = (\alpha_P)$ .*

Chamamos de espaço de adeles de  $F/K$  ao conjunto:

$$\mathcal{A}_F = \{\alpha; \alpha \text{ é adele de } F/K\}.$$

**Definição 1.6.3.** 1. *Definimos como adele principal de um elemento  $x \in F$  como sendo o adele cujas as componentes são todas iguais a  $x$  ou seja a seqüência constante  $(x)$ .*

2. Dado  $P \in \mathbb{P}_F$  e  $x \in F$ , o adele cuja as componentes são nulas a menos da componente  $P$ , a qual é  $x$ , será denotado por  $\iota_P(x)$ .

**Definição 1.6.4.** A um adele  $\alpha$ , associamos uma função de valorização discreta dada por:  $v_P(\alpha) := v_P(\alpha_P)$ .

**Definição 1.6.5.** Para um divisor  $A \in \mathcal{D}_F$  definimos o conjunto:

$$\mathcal{A}_F(A) = \{\alpha \in \mathcal{A}_F; v_P(\alpha) \geq -v_P(A), \forall P \in \mathbb{P}_F\}.$$

Facilmente pode se ver que o conjunto acima definido é um  $K$ -subespaço vetorial de  $\mathcal{A}_F$ .

No próximo teorema explicitamos um espaço vetorial cuja a dimensão é o índice de especialidade do divisor  $A$ .

**Teorema 1.6.6.** Dado um divisor  $A$ , o seu índice de especialidade é dado por:

$$i(A) = \dim_K(\mathcal{A}_F/(\mathcal{A}_F(A) + F)).$$

E como consequência imediata temos:

**Corolário 1.6.7.**

$$g = \dim_K(\mathcal{A}_F/(\mathcal{A}_F(0) + F)).$$

Agora veremos o conceito de diferenciais de Weil, o qual nos dará mais informações sobre o índice de especialidade de um divisor.

**Definição 1.6.8.** Uma aplicação  $K$ -linear,  $\omega : \mathcal{A}_F \rightarrow K$ , que se anula em  $\mathcal{A}_F(A) + F$  para algum divisor  $A \in \mathcal{D}_F$  é dita diferencial de Weil de  $F/K$ . Denotamos por  $\Omega_F$  ao conjunto dos diferenciais de Weil de  $F/K$  e por  $\Omega_F(A)$  ao conjunto de diferenciais de Weil de  $F/K$  que se anulam em  $\mathcal{A}_F(A) + F$ .

O conceito de divisor canônico é de fundamental importância para o Teorema de Riemann-Roch e ele é definido a partir da próxima definição e do lema seguinte.

**Definição 1.6.9.** Para um diferencial de Weil  $\omega \neq 0$  definimos o conjunto de divisores:

$$M(\omega) = \{A \in \mathcal{D}_F; \omega \text{ se anula em } \mathcal{A}_F(A) + F\}.$$

**Lema 1.6.10.** *Seja  $\omega \in \Omega_F$ ,  $\omega \neq 0$ , então existe um único divisor  $W \in M(\omega)$  tal que  $A \leq W$  para todo  $A \in M(\omega)$ .*

**Definição 1.6.11** (Divisor Canônico). 1. *O divisor  $(\omega)$  de um diferencial de Weil  $\omega \neq 0$  é o divisor de  $F/K$  unicamente determinado por:*

- (a)  $\omega$  se anula em  $\mathcal{A}_F((\omega)) + F$ ;
- (b) Se  $\omega$  se anula em  $\mathcal{A}_F(A) + F$  então  $A \leq (\omega)$ .

- 2. Para  $0 \neq \omega \in \Omega_F$  e  $P \in \mathbb{P}_F$  definimos  $v_P(\omega) = v_P((\omega))$ ;
- 3. Um lugar  $P$  é dito zero (resp. pólo) de  $\omega$  se  $v_P(\omega) > 0$  (resp.  $v_P(\omega) < 0$ ).  $\omega$  é chamado de regular em  $P$  se  $v_P(\omega) \geq 0$ , e simplesmente de regular se for regular em todos os lugares em  $\mathbb{P}_F$ ;
- 4. Um divisor  $W$  é dito divisor canônico de  $F/K$  se  $W = (\omega)$  para algum  $\omega \in \Omega_F$ .

**Proposição 1.6.12.** 1. Para  $0 \neq x \in F$  e  $0 \neq \omega \in \Omega_F$  temos que  $(x\omega) = (x) + (\omega)$ ;

2. Quaisquer dois divisores canônicos são equivalentes.

Esse próximo teorema vai nos permitir calcular o índice de especialidade de um divisor (mais uma vez como dimensão de um espaço vetorial).

**Teorema 1.6.13.** *Seja  $A$  um divisor arbitrário e  $W = (\omega)$  um divisor canônico de  $F/K$ . Então a aplicação*

$$\begin{aligned} \mu : \mathcal{L}(W - A) &\rightarrow \Omega_F(A) \\ x &\mapsto x\omega \end{aligned},$$

*é um isomorfismo de  $K$ -espaços Vetoriais, e mais  $i(A) = \dim(W - A)$ .*

Em fim chegamos ao principal teorema da teoria até aqui apresentada.

**Corolário 1.6.14** (Riemann-Roch). *Seja  $W$  um divisor canônico de  $F/K$ . Assim para qualquer  $A \in \mathcal{D}_F$  temos que:*

$$\dim(A) = \text{gr}(A) + 1 - g + \dim(W - A).$$

**Teorema 1.6.15.** *Sendo  $A$  um divisor de  $F/K$  de grau maior ou igual que  $2g-1$ , temos:*

$$\dim(A) = \text{gr}(A) + 1 - g.$$

A próxima definição nos será bastante útil para o entendimento de um de nossos códigos.

**Definição 1.6.16** (Componente Local). *Seja um diferencial de Weil  $\omega \in \Omega_F$ . Definimos a componente local de  $\omega$  como sendo a aplicação  $K$  – linear*

$$\begin{aligned} \omega_P : F &\rightarrow K \\ x &\mapsto \omega(\iota_P(x)) \end{aligned}.$$

Sobre as componentes locais temos os seguintes resultados:

**Proposição 1.6.17.** *Sejam um diferencial de Weil  $\omega \in \Omega_F$  e um adele  $\alpha = (\alpha_P) \in \mathcal{A}_F$ . Então  $\omega_P(\alpha_P) \neq 0$  no máximo em finitos lugares  $P$ , e mais,*

$$\omega(\alpha) = \sum_{P \in \mathbb{P}_F} \omega_P(\alpha_P).$$

*Em particular,*

$$\sum_{P \in \mathbb{P}_F} \omega_P(1) = 0.$$

O próximo resultado nos mostra que um diferencial de Weil é unicamente determinado em relação aos seus componentes locais.

**Proposição 1.6.18.** *1. Seja  $\omega \neq 0$  um diferencial de Weil de  $F/K$ ,  $P \in \mathbb{P}_F$  e  $W = (\omega)$ . Então:*

$$v_P(W) = \max\{r \in \mathbb{Z}; \omega_P(x) = 0 \text{ para todo } x \in F \text{ com } v_P(x) \geq -r\}.$$

*2. Se  $\omega, \omega' \in \Omega_F$  e  $\omega_P = \omega'_P$  para algum  $P \in \mathbb{P}_F$ , então  $\omega = \omega'$ .*

## 1.7 Curvas Algébricas

Nessa seção apresentaremos as curvas algébricas e sua ligação com os corpos de funções algébricas.

**Definição 1.7.1.** *Seja  $I$  um ideal em  $\mathbb{F}[x_1, \dots, x_n]$  (anel de polinômios em  $n$  indeterminadas com coeficientes sobre um corpo  $\mathbb{F}$ ). Definimos o conjunto algébrico obtido a partir de  $I$  como sendo:*

$$V(I) = \{a = (a_1, \dots, a_n) \in \mathbb{F}^n; f(a) = 0, \forall f \in I\}.$$

Dizemos que um conjunto algébrico  $B$  é irredutível se não pode ser escrito como união de dois outros conjuntos algébricos próprios. Temos que  $V(I)$  é irredutível quando o radical de  $I$  é ideal primo. Tal resultado nos leva as duas definições abaixo:

**Definição 1.7.2.** 1. *Dado um ideal primo  $I \subset \mathbb{F}[x_1, \dots, x_n]$  o conjunto  $\mathcal{X} = V(I)$  é dito variedade afim.*

2. *O anel  $\mathbb{F}[x_1, \dots, x_n]/I = \mathbb{F}[\mathcal{X}]$  é dito anel de coordenadas de  $\mathcal{X}$ .*

**Definição 1.7.3.** *Dada uma variedade algébrica  $\mathcal{X}$  definimos o corpo de funções racionais de  $\mathcal{X}$  como sendo o corpo de frações do anel de coordenadas  $\mathbb{F}[\mathcal{X}]$  que é denotado por  $\mathbb{F}(\mathcal{X})$ .*

Um resultado clássico da álgebra comutativa (Teorema de normalização de Noether) nos diz que podemos dar a dimensão da variedade algébrica da seguinte forma:

**Definição 1.7.4.** *Definimos a dimensão da variedade  $\mathcal{X}$  como sendo o grau de transcendência de  $\mathbb{F}(\mathcal{X})/\mathbb{F}$ .*

Para um ponto  $P \in \mathcal{X}$ , o conjunto

$$\mathcal{O}_P(\mathcal{X}) = \left\{ f \in \mathbb{F}(\mathcal{X}); f = \frac{g}{h}, g, h \in \mathbb{F}[\mathcal{X}] \text{ e } h(P) \neq 0 \right\},$$

é um anel local que tem como corpo de frações o próprio  $\mathbb{F}(\mathcal{X})$  e mais o seu ideal maximal é dado por:

$$M_P(\mathcal{X}) = \left\{ f \in \mathbb{F}(\mathcal{X}); f = \frac{g}{h}, g, h \in \mathbb{F}[\mathcal{X}], g(P) = 0 \text{ e } h(P) \neq 0 \right\}.$$

### 1.7.1 Variedades Projetivas

**Definição 1.7.5.** Dado um corpo  $\mathbb{F}$ , no conjunto  $\mathbb{F}^{n+1} \setminus \{0\}$  definimos a relação de equivalência  $\sim$  definida por: dados dois vetores  $v = (v_0, v_1, \dots, v_n)$  e  $w = (w_0, w_1, \dots, w_n) \in \mathbb{F}^{n+1} \setminus \{0\}$  eles são equivalentes se forem linearmente dependentes sobre  $\mathbb{F}$ , ou seja,  $v \sim w$  se, e somente se, existe  $\lambda \in \mathbb{F}$  tal que  $v = \lambda w$ .

O conjunto quociente  $(\mathbb{F}^{n+1} \setminus \{0\})/\sim$  das classes de equivalência segundo a relação  $\sim$ , é chamado **espaço projetivo de dimensão  $n$**  e denotado por  $\mathbf{P}^n(\mathbb{F})$  e seus elementos são denotados por  $(a_0 : a_1 : \dots : a_n)$ .

**Definição 1.7.6.** Dizemos que um polinômio  $F \in \mathbb{F}[x_1, \dots, x_n]$  é homogêneo se esse for soma de monômios de mesmo grau. Um ideal gerado por polinômios homogêneos é chamado de **ideal homogêneo**.

Observe que dados um ponto  $P = (a_0 : a_1 : \dots : a_n) = (b_0 : b_1 : \dots : b_n) \in \mathbf{P}^n(\mathbb{F})$  e um polinômio homogêneo  $F \in \mathbb{F}[x_0, \dots, x_n]$  podemos definir  $F(P) = 0$  se  $F(a_0, a_1, \dots, a_n) = 0$ , já que  $F(a_0, a_1, \dots, a_n) = 0$  se, e somente se,  $F(b_0, b_1, \dots, b_n) = 0$ . Assim, podemos definir o que seja uma variedade algébrica projetiva.

**Definição 1.7.7.** Um subconjunto  $\mathcal{X} \subset \mathbf{P}^n(\mathbb{F})$  é dito uma **variedade algébrica projetiva** se for o conjunto de zeros de um ideal homogêneo  $I \subset \mathbb{F}[x_0, x_1, \dots, x_n]$ , ou seja:

$$\mathcal{X} = V(I) = \{P \in \mathbf{P}^n(\mathbb{F}); F(P) = 0, \forall F \in I\}.$$

Uma variedade algébrica projetiva  $\mathcal{X} = V(I)$  é irredutível se, e somente se, o ideal  $I$  for um ideal homogêneo e o seu radical for primo.

O anel de coordenadas  $\mathbb{F}_h[\mathcal{X}] = \mathbb{F}[x_0, \dots, x_n]/I$  é dito anel de coordenadas homogêneas e os elementos que são do formato  $f = F + I$  com  $F \in \mathbb{F}[x_0, \dots, x_n]$  e  $F$  homogênea, são chamados de **forma de grau  $d$**  onde  $d = \text{gr}(F)$ .

Faremos agora a associação entre as curvas algébricas e os corpos de funções.

**Definição 1.7.8.** Se  $\mathcal{X}$  é uma variedade algébrica projetiva definimos o corpo de funções de  $\mathcal{X}$  como sendo:

$$\mathbb{F}(\mathcal{X}) = \left\{ \frac{g}{h}; g, h \in \mathbb{F}_h[\mathcal{X}] \text{ formas de mesmo grau e } h \neq 0 \right\}.$$

A dimensão da variedade  $\mathcal{X}$  é dada pelo grau de transcendência de  $\mathbb{F}(\mathcal{X})/\mathbb{F}$ .

**Definição 1.7.9.** *Dado um ponto  $P \in \mathcal{X}$  e  $f = \frac{g}{l} \in \mathbb{F}(\mathcal{X})$  com  $g, l \in \mathbb{F}_h[\mathcal{X}]$ , dizemos que  $f$  está definida em  $P$  se  $l(P) \neq 0$ ,  $f(P)$  é dito valor de  $f$  em  $P$ .*

O anel  $\mathcal{O}_P(\mathcal{X}) = \{f \in \mathbb{F}(\mathcal{X}); f \text{ é definida em } P\} \subset \mathbb{F}(\mathcal{X})$  é um anel local com ideal maximal  $M_P(\mathcal{X}) = \{f \in \mathcal{O}_P(\mathcal{X}); f(P) = 0\}$ .

**Definição 1.7.10.** *Seja  $F \in \mathbb{F}[x_1, \dots, x_n]$  com grau total de  $F$  igual a  $l$ , definimos a homogeneização de  $F$  como sendo:*

$$F^* = x_0^l F\left(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}\right).$$

**Definição 1.7.11.** *Uma variedade projetiva (afim)  $\mathcal{X}$  de dimensão 1 é chamada de curva algébrica irredutível projetiva (afim). Desse modo o corpo de funções racionais em  $\mathcal{X}$ ,  $\mathbb{F}(\mathcal{X})$ , é um corpo de funções algébricas de uma variável como na definição 1.3.1. Mais ainda, dizemos que a curva algébrica projetiva (afim) é plana se  $\mathcal{X} \subset \mathbb{P}^2(\mathbb{F})$  (ou  $\mathbb{F}^2$ ).*

## 1.7.2 Curvas Não Singulares

Levando-se em conta que os códigos geométricos de Goppa são gerados pelas curvas planas não singulares, a seguir apresentaremos a definição de curvas não singulares.

**Definição 1.7.12.** *Seja  $\mathcal{X}$  uma curva algébrica definida pelo polinômio  $F \in \mathbb{F}(x, y)$  e  $P$  um ponto em  $\mathcal{X}$ . Dizemos que o ponto  $P$  é um ponto não singular se pelo menos uma das derivadas parciais de  $F$  aplicadas nesse ponto é não nula, ou seja,  $F_x(P) \neq 0$  ou  $F_y(P) \neq 0$ . Se todos os pontos da curva forem não singulares dizemos apenas que a curva é não singular (ou regular).*

Observamos que aqui que a derivada parcial de um polinômio é a sua derivada formal.

## Capítulo 2

# Códigos Algébricos Geométricos

Neste capítulo estamos interessados em construir os códigos algébricos geométricos, conhecidos como Códigos de Goppa Geométricos, e então extrair uma cota para a sua distância mínima e calcular sua dimensão. Aqui  $\mathbb{F}_q$  denotará um corpo com  $q$  elementos.

### 2.1 Códigos Algébricos Geométricos

**Definição 2.1.1.** *Seja  $\mathbb{F}_q = \{\alpha_0, \dots, \alpha_{q-1}\}$  e considere o conjunto,  $\mathcal{L}_k \subset \mathbb{F}_q[x]$ , dos polinômios com grau menor que  $k$  e  $k \leq q$ , definimos um código de Reed-Solomon de tamanho  $n = q$  como sendo:*

$$C_k = \{c(f) = (f(\alpha_0), \dots, f(\alpha_{q-1})); f \in \mathcal{L}_k\}.$$

**Proposição 2.1.2.** *Como acima definido,  $C_k$  é um código MDS (Maximum Distance Separable), ou seja, tem distância mínima  $d = n - k + 1$ .*

*Demonstração.* Seja  $f \in \mathcal{L}_k$ , temos que  $f$  tem grau no máximo  $k - 1$ , assim  $f$  admite no máximo  $k - 1$  raízes distintas em  $\mathbb{F}_q$ , desse modo o peso de  $c(f)$  é no mínimo  $n - k + 1$ , ou seja,  $d \geq n - k + 1$  no entanto temos que o polinômio  $g(x) = (x - \alpha_{i_1}) \cdots (x - \alpha_{i_{k-1}}) \in \mathcal{L}_k$  tem grau  $k - 1$  e tem exatamente  $k - 1$  raízes distintas em  $\mathbb{F}_q$ , desse modo  $d(c(g)) = n - k + 1$ .  $\square$

A seguir utilizaremos as seguintes notações:



- ★  $F/\mathbb{F}_q$ , um corpo de funções algébricas de gênero  $g$ ;
- ★  $P_1, P_2, \dots, P_n$ , lugares de grau 1 dois a dois distintos em  $F/\mathbb{F}_q$ ;
- ★  $D = \sum_{i=1}^n P_i$ , um divisor em  $F/\mathbb{F}_q$ ;
- ★  $G$ , um divisor em  $F/\mathbb{F}_q$  tal que  $\text{supp}(G) \cap \text{supp}(D) = \emptyset$ .

A partir das notações dadas acima e da definição 1.3.11 estamos em condição de definir o que vem a ser um código gemétrico de Goppa.

**Definição 2.1.3** (Códigos Geométricos de Goppa). *Definimos o código algébrico geométrico (código geométrico de Goppa) associado aos divisores  $D$  e  $G$  como sendo:*

$$C(D, G) = \{c(x) = (x(P_1), x(P_2), \dots, x(P_n)); x \in \mathcal{L}(G)\}.$$

**Teorema 2.1.4.** *O código de Goppa  $C(D, G)$  é um  $[n, k, d]$ -código tal que:*

$$k = \dim(G) - \dim(G - D) \text{ e } d \geq n - \text{gr}(G).$$

*Demonstração.* Seja a aplicação de avaliação

$$\begin{aligned} \text{ev}_D : \mathcal{L}(G) &\rightarrow C(D, G) \\ x &\mapsto c(x) = ((x(P_1), \dots, x(P_n))) \end{aligned}$$

Sabemos que  $\text{ev}_D$  é sobrejetiva logo  $\frac{\mathcal{L}(G)}{\text{Ker}(\text{ev}_D)} \simeq C(D, G)$ . Queremos agora mostrar que  $\text{Ker}(\text{ev}_D) = \mathcal{L}(G - D)$ . Seja  $x \in \text{Ker}(\text{ev}_D)$ , temos que para todo  $Q \in \mathbb{P}_F$   $v_Q(x) \geq -v_Q(G)$  e  $v_{P_i}(x) > 0$  para  $i = 1, \dots, n$  e mais, como  $\text{supp}(G) \cap \text{supp}(D) = \emptyset$ , temos que,  $v_Q(x) \geq -v_Q(G) + v_Q(D)$  assim  $\text{Ker}(\text{ev}_D) \subset \mathcal{L}(G - D)$ .

Tomemos agora  $x \in \mathcal{L}(G - D)$ , temos que  $v_{P_i}(x) \geq -v_{P_i}(G) + v_{P_i}(D) = 1$  para  $i = 1, \dots, n$ , logo  $x \in \mathcal{L}(G)$  e  $v_{P_i}(x) > 0$  ou seja  $x(P_i) = 0$  em  $F_{P_i}$  o que implica que  $\mathcal{L}(G - D) \subset \text{Ker}(\text{ev}_D)$  e pelo teorema dos isomorfismos (álgebra linear) concluímos que  $k = \dim(G) - \dim(G - D)$ .

Agora acharemos uma cota para a distância mínima do código. Assumiremos que  $C(D, G) \neq \{0\}$ , pois caso contrário não teríamos uma distância não nula.

Seja  $x \in C(D, G)$  tal que  $w(x) = d$ , assim temos que existe  $y \in \mathcal{L}(G)$  tal que  $w(ev_D(y)) = d$ , mas  $w(ev_D(y)) = d = \#\{i; y(P_i) \neq 0\}$ . Suponha agora que  $y(P_1) = y(P_2) = \dots = y(P_{n-d}) = 0$ , reordenando os  $P_i$ 's caso necessário, logo

$$\begin{aligned} 0 \neq y \in \mathcal{L}\left(G - \sum_{i=1}^{n-d} P_i\right) &\Rightarrow \dim\left(G - \sum_{i=1}^{n-d} P_i\right) \neq 0 \Rightarrow \\ 0 &\leq gr\left(G - \sum_{i=1}^{n-d} P_i\right) = gr(G) - n + d \Rightarrow \\ d &\geq n - gr(G). \end{aligned}$$

□

**Corolário 2.1.5.** *Suponha que  $gr(G) < n$  então  $ev_D : \mathcal{L}(G) \rightarrow C(D, G)$  é injetora e se  $2g - 2 < gr(G) < n$  teremos que  $k = gr(G) + 1 - g$ .*

*Demonstração.* Temos que  $gr(G - D) = gr(G) - n < 0$ , logo (por 1.5.8-2)  $\{0\} = \mathcal{L}(G - D) = Ker(ev_D)$  logo  $ev_D$  é injetora. Pelo teorema 1.6.15 temos que  $k = gr(G) + 1 - g$ . □

Esses resultados dão uma motivação para a seguinte definição:

**Definição 2.1.6.** *No código geométrico de Goppa  $C(D, G)$  chamamos de distância designada ao inteiro  $d^* = n - gr(G)$ .*

Ao ver essa definição surge uma pergunta: Quando a distância designada é igual a distância mínima do código? Responderemos essa pergunta na próxima proposição.

**Proposição 2.1.7.** *Seja  $C(D, G)$  um código com distância designada  $d^*$ , suponha que  $\dim(G) > 0$  e que  $d^* > 0$ . então  $d = d^*$  se, e somente se, existe um divisor  $D'$  com  $0 \leq D' \leq D$ ,  $gr(D') = gr(G)$  e  $\dim(G - D') > 0$ .*

*Demonstração.* Suponha que  $d = d^*$ . Seja  $0 \neq x \in \mathcal{L}(G)$  tal que  $w(ev_D(x)) = d$ . Assim,  $ev_D(x) = (x(P_1), \dots, x(P_n))$ , reordenando os  $P_i$ 's caso necessário, temos  $x(P_1) = \dots = x(P_{gr(G)}) = 0$ . Seja  $D' = \sum_{i=1}^{gr(G)} P_i$ , logo  $gr(D') = \sum_{i=1}^{gr(G)} v_{P_i}(D') = gr(G)$ . Assim temos que  $0 \leq D' \leq D$ . Observe que  $x \in Ker(ev_{D'})$  logo como na demonstração do teorema 2.1.4, tem-se  $\dim(G - D') > 0$ .

Queremos agora demonstrar a segunda parte da proposição. Seja  $D' \in \mathcal{D}_F$  tal que  $0 \leq D' \leq D$ ,  $gr(D') = gr(G)$  e  $dim(G - D') > 0$ , então temos que existe  $y \in \mathcal{L}(G - D')$ , assim sendo, temos que o peso da palavra código  $(y(P_1), \dots, y(P_n))$  é no máximo  $n - gr(G) = d^*$ , contudo  $d$  é a distância mínima no código e mais, como provado anteriormente  $d^* \leq d$ , logo  $d = d^*$ .  $\square$

Agora definiremos o código que originalmente foi introduzido por V. D. Goppa em 1981 no artigo “Codes on Algebraic Curves”.

**Definição 2.1.8.** *Seja  $G$  e  $D = P_1 + \dots + P_n$  divisores de  $F/\mathbb{F}_q$  com os  $P_i$ 's dois a dois disjuntos e  $supp(G) \cap supp(D) = \emptyset$ . Definimos o código  $C_\Omega(D, G)$  por:*

$$C_\Omega = \{(\omega_{P_1}(1), \dots, \omega_{P_n}(1)) \in \mathbb{F}_q^n; \omega \in \Omega(G - D)\}.$$

O próximo resultado tem como objetivo caracterizar o código  $C_\Omega(D, G)$ . Mas antes disso apresentaremos um lema técnico.

**Lema 2.1.9.** *Sejam  $F/\mathbb{F}_q$  um corpo de funções,  $P \in \mathbb{P}_F$  com  $gr(P) = 1$  e  $\omega \in \Omega_F$  um diferencial de Weil tal que  $v_P(\omega) \geq -1$ . Então  $\omega_P(1) = 0$  se, e somente se,  $v_P(\omega) \geq 0$ .*

*Demonstração.*  $\Leftarrow$ ) Primeiro vamos supor que  $v_P(\omega) \geq 0$ , logo pela proposição 1.6.18, temos que  $\omega_P(x) = 0$  para todo  $x \in F$  com  $v_P(x) \geq 0$ , temos que  $1 \in \mathbb{F}_q \subset F$  logo  $v_P(1) = 0$  assim  $\omega_P(1) = 0$ .

$\Rightarrow$ ) Suponha agora que  $\omega_P(1) = 0$ , assim temos que  $\omega_P(a) = a\omega_P(1) = 0$  para todo  $a \in \mathbb{F}_q$ . Pelo teorema 1.3.14, existe  $x \in F$  tal que  $v_P(x) \geq 0$ , ou seja  $x \in \mathcal{O}_P$ . Como  $gr(P) = 1$  temos que  $\mathcal{O}_P/P = \mathbb{F}_q$ , assim existem  $y \in P$  e  $a \in \mathbb{F}_q$  tais que  $x - y = a$  e mais,  $v_P(y) \geq 1$  e  $v_P(a) = 0$ . Por hipótese temos que  $v_P(\omega) \geq -1$  e como  $v_P(y) \geq 1$ , pela proposição 1.6.18, temos que  $\omega_P(y) = 0$ . Assim temos que  $\omega_P(x) = \omega_P(a + y) = \omega_P(a) + \omega_P(y) = 0$ , ou seja,  $v_P(\omega) \geq 0$  (novamente pela proposição 1.6.18).  $\square$

**Observação 2.1.10.** *A proposição 1.6.18 nos garante que  $v_P(\omega) \geq r$  se, e somente se,  $\omega(x) = 0$  para todo  $x \in F$  com  $v_P(x) \geq -r$ .*

Agora enuciaremos o teorema que caracteriza o código  $C_\Omega(D, G)$ .

**Teorema 2.1.11.** *O código  $C_\Omega(D, G)$  é um  $[n, k', d']$ -código com parâmetros:*

$$k' = i(G - D) - i(G) \text{ e } d' \geq gr(G) - 2g + 2.$$

*E mais, se  $gr(G) > 2g - 2$ , temos que  $k' = i(G - D) \geq n + g - 1 - gr(G)$  e se  $2g - 2 < gr(G) < n$  então  $k' = n + g - 1 - gr(G)$ .*

*Demonstração.* Seja  $\phi$  a seguinte aplicação:

$$\begin{aligned} \phi: \Omega_F(G - D) &\rightarrow C_\Omega(D, G) \\ \omega &\mapsto (\omega_{P_1}(1), \dots, \omega_{P_n}(1)) \end{aligned}$$

obviamente  $\phi$  é sobrejetiva, logo  $C_\Omega(D, G)$  é isomorfo a  $\Omega_F(G - D)/Ker(\phi)$ .

Seja  $\omega \in Ker(\phi)$ , temos que  $\omega_{P_i}(1) = 0$  para  $i = 1 \dots n$ , assim pelo lema 2.1.9,  $v_{P_i}(\omega) \geq 0$ . Como  $\omega \in \Omega_F(G - D)$ , temos que  $(\omega) \geq G - D$ . Observe que se  $P \in \{P_1, \dots, P_n\}$  temos que  $v_P(G) = 0$  e  $v_P(-d) < 0$  e mais, para  $P \notin \{P_1, \dots, P_n\}$  temos que  $v_P(-D) = 0$  assim  $\omega \in \Omega_F(G)$ .

Seja agora  $\omega \in \Omega_F(G)$ , novamente pelo lema 2.1.9 temos que  $v_{P_i}(\omega) \geq v_{P_i}(G) = 0$ , logo  $\omega \in Ker(\phi)$ .

Assim pelo isomorfismo visto acima temos que

$$k' = \dim_{\mathbb{F}_q}(\Omega_F(G - D)) - \dim_{\mathbb{F}_q}(\Omega_F(G)) = i(G - D) - i(G).$$

Seja  $\phi(\omega) \in C_\Omega(D, G)$ , uma palavra com peso  $m > 0$ , sem perda de generalidade podemos supor que  $v_{P_1} = \dots = v_{P_{n-m}}$ , desse modo temos que  $\omega \in \Omega_F(G - (D - \sum_{i=1}^{n-m} P_i))$ .

Observe que  $i(G - (D - \sum_{i=1}^{n-m} P_i)) = \dim_{\mathbb{F}_q}(G - (D - \sum_{i=1}^{n-m} P_i))$  e como  $\Omega(G - (D - \sum_{i=1}^{n-m} P_i)) \neq \{0\}$  temos que  $i(G - (D - \sum_{i=1}^{n-m} P_i)) > 0$ , desse modo  $\dim(G - (D - \sum_{i=1}^{n-m} P_i)) > gr(G - (D - \sum_{i=1}^{n-m} P_i)) - g + 1$  o que é a contra positiva do teorema 1.6.15, assim

$$2g - 2 \geq gr\left(G - \left(D - \sum_{i=1}^{n-m} P_i\right)\right) = gr(G) - gr\left(D - \sum_{i=1}^{n-m} P_i\right) = gr(G) - m$$

concluimos então que  $m \geq gr(G) - 2g + 2$ , ou seja,  $d' \geq gr(G) - 2g + 2$ .

Assuma agora que  $gr(G) > 2g - 2$ . Pelo teorema 1.6.15, temos que  $i(G) = 0$ , assim  $k' = i(G - D) = \dim(G - D) - gr(G - D) + g - 1$ , como  $\dim(G - D) \geq 0$  temos que  $k' \geq n + g - 1 - gr(G)$ .

Agora se  $gr(G) < n$  temos que  $gr(G - D) = gr(G) - n < 0$  logo pelo corolário 1.5.8  $dim(G - D) = 0$  assim  $k' = n + g - 1 - gr(G)$ .  $\square$

O próximo teorema mostra a ligação entre o código geométrico de Goppa ( $C(D, G)$ ) e o código que acabamos de definir  $C_\Omega(D, G)$ . Novamente antes do teorema apresentaremos mais um lema técnico.

**Lema 2.1.12.** *Sejam  $P \in \mathbb{P}_F$  tal que  $gr(P) = 1$ ,  $\omega$  um diferencial de Weil com  $v_P(\omega) \geq -1$  e  $x \in F$  com  $v_P(x) \geq 0$ , então*

$$\omega_P(x) = x(P)\omega_P(1).$$

*Demonstração.* Como  $gr(P) = 1$  temos que  $\mathcal{O}_P/P = \mathbb{F}_q$ , o fato de  $v_P(x) \geq 0$  nos dá que  $x \in \mathcal{O}_P$ , logo existe  $y \in P$  e  $a \in \mathbb{F}_q$  tais que  $x - y = a$ , observe que  $v_P(a) = 0$  e  $v_P(y) \geq 1$ . Como  $v_P(y) \geq 1$  temos que  $\omega_P(y) = 0$ , assim  $\omega_P(x) = \omega_P(a + y) = \omega_P(a) + \omega_P(y) = a\omega_P(1)$ .

Observe agora que  $a$  é a classe de resíduos de  $x$  em relação a  $P$ , logo  $\omega_P(x) = x(P)\omega_P(1)$ .  $\square$

Em fim o teorema que nos dá a relação entre os códigos.

**Teorema 2.1.13.** *Os códigos  $C(D, G)$  e  $C_\Omega(D, G)$  são duais entre si, ou seja,*

$$C_\Omega(D, G) = C(D, G)^\perp.$$

*Demonstração.* Primeiro vamos mostrar que a dimensão dos códigos  $(C(D, G))^\perp$  e  $C_\Omega(D, G)$  são iguais.

Pelo teorema 2.1.11 temos que  $dim(C_\Omega(D, G)) = i(G - D) - i(G)$ , agora pelo corolário 1.6.14 (Riemann-Rock) temos que  $i(G - D) - i(G) = dim(G - D) + g - 1 - gr(G - D) - (dim(G) + g - 1 - gr(G)) = dim(G - D) + gr(D) - dim(G) = n + dim(G - D) - dim(G)$ , pelo teorema 2.1.4 temos que  $dim(C(D, G)) = dim(G) - dim(G - D)$ , assim  $dim(C_\Omega(D, G)) = dim(C(D, G)^\perp)$ .

Agora mostraremos que  $C_\Omega(D, G) \subset C(D, G)^\perp$ , o que vai nos garantir a igualdade desejada.

Seja  $\omega \in \Omega_F(G - D)$  e  $x \in \mathcal{L}(G)$ . Identificando  $x$  como um adele principal temos que  $0 = \omega(x) = \sum_{P \in \mathbb{P}_F} \omega_P(x)$  (pela proposição 1.6.17). Para  $P \in$

$\mathbb{P}_F \setminus \{P_1, \dots, P_n\}$  temos que  $v_P(x) \geq -v_P(\omega)$ , então pela observação 2.1.10 temos que  $v_P(x) = 0$ , assim  $\sum_{P \in \mathbb{P}_F} \omega_P(x) = \sum_{i=1}^n \omega_{P_i}(x)$ . Agora pelo lema 2.1.12 temos que  $\sum_{i=1}^n \omega_{P_i}(x) = \sum_{i=1}^n x(P_i) \omega_{P_i}(1) = \langle (\omega_{P_1}, \dots, \omega_{P_n}), (x(P_1), \dots, x(P_n)) \rangle$ , concluindo então que  $C_\Omega(D, D) \subset C(D, G)^\perp$ .  $\square$

## 2.2 Teorema de Bézout

Nesta seção ficaremos a par do teorema de Bézout, o qual fala sobre o número de interseções entre curvas algébricas e também o ligaremos a teoria de códigos, foco deste trabalho.

**Teorema 2.2.1** (Teorema de Bézout). *Sejam  $\mathcal{X}$  e  $\mathcal{Y}$  duas curvas algébricas planas irredutíveis de grau  $l$  e  $m$  respectivamente sobre um corpo algebricamente fechado  $\mathbb{F}$  tais que elas não tenham uma componente em comum, então o número de pontos da interseção entre as curvas é exatamente  $lm$  (contando os pontos com suas multiplicidades).*

*Demonstração.* A demonstração desse resultado não está no objetivo desse texto, contudo ela se encontra em [1].  $\square$

**Proposição 2.2.2.** *Consideremos um polinômio  $G \in \mathbb{F}_q[x, y]$  com grau total  $m$  tal que sua forma homogênea  $G^*$  define uma curva irredutível não singular  $\mathcal{X}$ , então  $G$  é irredutível em  $\mathbb{F}[x, y]$ , onde  $\mathbb{F}$  é o fecho algébrico de  $\mathbb{F}_q$ .*

*Demonstração.* Pela nossa definição  $\mathcal{X}$  é uma curva gerada por um ideal primo  $I \subset \mathbb{F}[x, y, z]$  e mais  $I = \langle G^* \rangle$ . Logo  $G^*$  é irredutível em  $\mathbb{F}[x, y, z]$ . Agora sendo  $G^*$  irredutível e supondo, por absurdo, que  $G$  seja redutível temos que  $G = fh$  com  $gr(f) < gr(G)$  e  $gr(h) < gr(G)$ , logo temos que  $G^* = (fh)^* = f^*g^*$  que é redutível, absurdo, assim temos que  $G$  é irredutível em  $\mathbb{F}[x, y]$ .  $\square$

**Definição 2.2.3.** *Seja  $\mathcal{X}$  uma curva definida sobre  $\mathbb{F}_q$ , isto é, as equações que a define tem seus coeficientes em  $\mathbb{F}_q$ . Os pontos de  $\mathcal{X}$  que tem todas as coordenadas em  $\mathbb{F}_q$  são ditos pontos racionais.*

Seja  $V_l$  o espaço vetorial de polinômios de grau total no máximo  $l$ , em duas variáveis  $x, y$  e com coeficientes em  $\mathbb{F}_q$ . Considere  $G$  um polinômio como o da

proposição 2.2.2 (em particular, o grau total de  $G$  é  $m$ ),  $P_1, P_2, \dots, P_n$  pontos racionais da curva definida por  $G$ . Definimos o código  $C$  por:

$$C = \{(f(P_1), f(P_2), \dots, f(P_n)); f \in V_l\}.$$

**Teorema 2.2.4.** *Se no código  $C$ , definido acima tem-se que  $n > lm$ , então para sua distância mínima  $d$  e sua dimensão  $k$  são dadas por:*

$$d \geq n - lm;$$

$$k = \begin{cases} \binom{l+2}{2}, & \text{se } l < m; \\ lm + 1 - \binom{m-1}{2}, & \text{se } l \geq m. \end{cases}$$

*Demonstração.* Primeiro queremos encontrar a dimensão do espaço vetorial  $V_l$  que tem como base o conjunto formado pelo monômios de grau menor ou igual a  $l$ , conjunto esse que tem cardinalidade igual a  $\sum_{i=0}^l (l+1-i) = \frac{2(l+1)^2 - (l+1)l}{2} = \frac{(l+1)(l+2)}{2} = \binom{l+2}{2}$ , assim a dimensão de  $V_l$  é  $\binom{l+2}{2}$ .

Seja  $F \in V_l$ , se  $G$  for um fator de  $F$  temos que a palavra correspondente a  $F$  no código é zero. Agora dada uma palavra nula no código e  $F \in V_l$  o polinômio que a gera temos que a curva  $\mathcal{Y}$  definida por  $F = 0$  e  $G = 0$  tem grau  $l' \leq l$  e  $l' \leq m$  e mais, temos que  $P_1, \dots, P_n$  estão na interseção de  $\mathcal{Y}$  com  $\mathcal{X}$ . O teorema de Bézout nos garante que se  $\mathcal{Y}$  e  $\mathcal{X}$  não tem um fator em comum o número de pontos na interseção é menor ou igual a  $l'm \leq lm$ , mas por hipótese  $n > lm$ , logo  $F$  tem  $G$  como seu fator. Assim temos que as funções em  $V_l$  que geram a palavra zero é um subespaço vetorial de dimensão  $l - m$  dado por  $GV_{l-m} = \{GH; H \in V_{l-m}\}$ .

Se  $l < m$  temos que  $V_{l-m} = \emptyset$  logo a dimensão do código é dada por  $k = \binom{l+2}{2}$ . Caso contrário, teremos que  $k = \binom{l+2}{2} - \binom{l-m+2}{2} = lm + 1 - \binom{m-1}{2}$ .

Agora queremos demonstrar que a distância mínima do código é  $d \geq n - lm$ . De fato, seja  $w \in C$  uma palavra não nula, suponha que  $w$  tem mais que  $lm$  coordenadas nulas. Seja  $F \in V_l$  um polinômio que gere  $w$ , tomemos a curva  $\mathcal{Y}$  definida por  $F = 0$ , como  $gr(F) \leq l$  temos que  $gr(\mathcal{Y}) \leq l$  logo  $\#\mathcal{Y} \cap \mathcal{X} \leq lm$ , pelo teorema de Bézout. Com um possível reordenamento das coordenadas de  $w$  podemos supor que  $F(P_1) = F(P_2) = \dots = F(P_{lm}) = \dots = F(P_j) = 0$ , pela nossa construção temos que  $\{P_1, \dots, P_j\} \subset \mathcal{Y} \cap \mathcal{X}$ . Logo  $j \leq lm$ , assim  $d \geq n - lm$ , como queríamos demonstrar.  $\square$

# Capítulo 3

## Códigos de Avaliação

Este capítulo está dedicado a construção dos códigos de avaliação.

### 3.1 Funções Peso, Grau e Ordem

**Definição 3.1.1.** *Seja  $R = \mathbb{F}[x_1, \dots, x_m]$  o anel de polinômios a  $m$  variáveis sobre o corpo  $\mathbb{F}$ , suponha que exista uma ordem total  $\prec$  no conjunto de monômios de  $R$  tal que para quaisquer monômios  $M_1$ ,  $M_2$  e  $M$  temos que:*

1. *Se  $M \neq 1$ , então  $1 \prec M$ ;*
2. *Se  $M_1 \prec M_2$ , então  $MM_1 \prec MM_2$ .*

*Assim dizemos que  $\prec$  é uma ordem de admissão ou ordem de redução em monômios.*

No que segue  $R$  é uma  $\mathbb{F}$ -álgebra, ou seja, um anel comutativo com unidade tal que  $\mathbb{F} \subset R$  como subanel. E mais, o símbolo  $-\infty$  é tal que para todo  $n \in \mathbb{N}_0 \cup \{-\infty\}$ ,  $-\infty + n = -\infty$ .

**Definição 3.1.2.** *Uma função  $\rho : R \rightarrow \mathbb{N}_0 \cup \{-\infty\}$ , que satisfaz as propriedades abaixo é chamada de **função ordem**.*

1.  $\rho(f) = -\infty$  se, e somente se,  $f = 0$ ;
2.  $\rho(\lambda f) = \rho(f)$  para todo  $\lambda \in \mathbb{F} \setminus \{0\}$ ;



3.  $\rho(f + g) \leq \max\{\rho(f), \rho(g)\}$  e a igualdade é válida quando  $\rho(f) \neq \rho(g)$ ;
4. Se  $\rho(f) < \rho(g)$  e  $h \neq 0$ , então  $\rho(fh) < \rho(gh)$ ;
5. Se  $\rho(f) = \rho(g) \neq 0$ , então existe  $\lambda \in \mathbb{F} \setminus \{0\}$  tal que  $\rho(f - \lambda g) < \rho(g)$ .

Se além dessas propriedades  $\rho$  também satisfizer a próxima a chamaremos de função peso.

6.  $\rho(fg) = \rho(f) + \rho(g)$ .

**Exemplo 3.1.3.** Um primeiro exemplo de uma função peso é a função grau de polinômios no anel de polinômios em uma variável  $\mathbb{F}[x]$ .

**Definição 3.1.4.** Uma função grau em  $R$  é uma função que satisfaz as propriedades 1, 2, 3, 4 e 6 da definição 3.1.2.

Vejamos agora um resultado que nos traz propriedades para as funções ordem.

**Lema 3.1.5.** Seja  $\rho$  uma função ordem em  $R$ , então temos:

1. Se  $\rho(f) = \rho(g)$ , então  $\rho(fh) = \rho(gh)$  para todo  $h \in R$ ;
2. Se  $f \in R \setminus \{0\}$ , então  $\rho(1) \leq \rho(f)$ ;
3.  $\mathbb{F} = \{f \in R; \rho(f) \leq \rho(1)\}$ ;
4. Se  $\rho(f) = \rho(g)$ , então existe um único escalar não nulo  $\lambda \in \mathbb{F}$  tal que  $\rho(f - \lambda g) < \rho(g)$ .

*Demonstração.* A demonstração desse lema sairá diretamente da definição de funções ordem.

(1) Seja  $\rho(f) = \rho(g)$ , temos que existe  $\lambda \in \mathbb{F}$  tal que  $\rho(f - \lambda g) < \rho(g)$ , logo  $\rho(fh - \lambda gh) < \rho(gh)$ . Podemos escrever  $fh = (fh - \lambda gh) + \lambda gh$ , assim  $\rho(fh) = \rho(\lambda gh) = \rho(gh)$ .

(2) Suponha por absurdo que  $f \in R$  é um elemento não nulo tal que  $\rho(f) < \rho(1)$ , então a cadeia  $\rho(1) > \rho(f) > \rho(f^2) > \dots$  é estritamente decrescente, absurdo, pois  $\mathbb{N}_0 \cup \{-\infty\}$  é bem ordenado.

(3) Claramente  $\mathbb{F} \subset H = \{f \in R; \rho(f) \leq \rho(1)\}$ , agora seja  $f \neq 0$  tal que  $\rho(f) \leq \rho(1)$  então  $\rho(f) = \rho(1)$ , assim existe  $\lambda$  tal que  $\rho(f - \lambda) < \rho(1)$ , logo  $f - \lambda = 0$  ou seja  $f \in \mathbb{F}$ .

(4) Pela definição de função ordem, temos a existência do  $\lambda$ , falta assim mostrar a unicidade. Suponha que  $\lambda, \nu \in \mathbb{F}$  são tais que  $\rho(f - \lambda g) < \rho(g)$  e  $\rho(f - \nu g) < \rho(g)$ . Então temos que  $\rho(f - \lambda g - (f - \nu g)) \leq \max\{\rho(f - \lambda g), \rho(f - \nu g)\} < \rho(g)$ . Assim temos que  $\rho((\lambda - \nu)g) < \rho(g)$  o que implica que  $\lambda - \nu = 0$ . Assim  $\lambda = \nu$ .  $\square$

Uma primeira consequência sobre a estrutura de um anel  $R$  com uma função ordem é dada na seguinte proposição:

**Proposição 3.1.6.** *Se existe uma função ordem,  $\rho$ , em  $R$ , então  $R$  é um domínio de integridade.*

*Demonstração.* Suponha que existam  $f, g \in R \setminus \{0\}$  tais que  $fg = 0$ , sem perda de generalidade assumiremos que  $\rho(f) \leq \rho(g)$ , assim  $\rho(f^2) \leq \rho(fg) = \rho(0) = -\infty$  logo  $\rho(f^2) = -\infty$ , isto é,  $f^2 = 0$ . Como  $f \neq 0$ , temos que  $\rho(1) \leq \rho(f) \leq \rho(f^2)$ , absurdo. Logo  $fg \neq 0$  assim  $R$  é um domínio.  $\square$

Agora apresentaremos um exemplo com o qual mostraremos que a recíproca da proposição 3.1.6 é falsa.

**Exemplo 3.1.7.** A  $\mathbb{F}$ -álgebra  $R = \mathbb{F}[x, y]/\langle xy - 1 \rangle$  é um domínio, mas não tem uma função ordem. De fato, denotando por  $\bar{x}$  a classe de equivalência  $x + \langle xy - 1 \rangle$  e por  $\bar{y}$  a classe  $y + \langle xy - 1 \rangle$ . Como  $R$  é um domínio temos que  $\bar{x} \neq 0$  e  $\bar{y} \neq 0$ . Sendo  $\rho$  uma função ordem em  $R$  temos que  $\rho(1) \leq \rho(\bar{x})$  e assim  $\rho(\bar{y}) \leq \rho(\bar{x}\bar{y}) = \rho(1)$ , ou seja,  $\rho(\bar{y}) = \rho(1)$ , analogamente achamos que  $\rho(\bar{x}) = \rho(1)$ . Observe que  $R = \mathbb{F}[\bar{x}] + \mathbb{F}[\bar{y}]$  e assim para todo  $f \in R$  concluimos que  $\rho(f) \leq \rho(1)$ , ou seja,  $R = \mathbb{F}$ , no entanto  $\bar{x} \notin \mathbb{F}$ , absurdo.

A seguir mostraremos que dada uma  $\mathbb{F}$ -álgebra  $R$  com uma função ordem, essa admite uma  $\mathbb{F}$ -base com “boas” propriedades.

**Teorema 3.1.8.** *Seja  $R$  uma  $\mathbb{F}$ -álgebra com uma função ordem  $\rho$ ,  $\mathbb{F} \neq R$ . Então:*

1. Existe uma  $\mathbb{F}$ -base,  $\{f_i, i \in \mathbb{N}\}$ , para  $R$  tal que  $\rho(f_i) < \rho(f_{i+1})$  para todo  $i \in \mathbb{N}$ ;
2. Se  $f = \sum_{i=1}^m \lambda_i f_i$  com  $\lambda_i \in \mathbb{F}$  e  $\lambda_m \neq 0$ , temos que  $\rho(f) = \rho(f_m)$ ;
3. Seja  $l(i, j) := l$  o inteiro tal que  $\rho(f_i f_j) = \rho(f_l)$ . Assim,  $l(i, j) < l(i+1, j)$  para todo  $i, j$ ;
4. Seja  $\rho_i := \rho(f_i)$ . Se  $\rho$  é uma função peso então  $\rho_{l(i,j)} = \rho_i + \rho_j$ .

*Demonstração.* (1) Temos que existe  $f \in R$  com  $f \notin \mathbb{F}$ , pois  $R \neq \mathbb{F}$ , assim  $\rho(1) < \rho(f)$  o que nos dá que  $\rho(f^n) < \rho(f^{n+1})$  para todo  $n \in \mathbb{N}_0$ . Mais ainda, o conjunto dos valores de  $\rho$  é infinito. Seja  $(\rho_i)_{i \in \mathbb{N}}$  a seqüência crescente de inteiros não negativos tais que os  $\rho_i$ 's são todos os valores da função ordem, isto é,  $\rho(R \setminus \{0\}) = \{\rho_i; i \in \mathbb{N}\}$ . Por definição, para todo  $i \in \mathbb{N}$  existe um  $f_i \in R$  tal que  $\rho(f_i) = \rho_i$  assim  $\rho(f_i) < \rho(f_{i+1})$ . E mais, pela nossa construção, para todo  $f \in R \setminus \{0\}$  existe um  $f_i$  tal que  $\rho(f) = \rho(f_i)$ . Observamos que  $\rho_1 = \rho(1)$ . Agora falta mostrar que  $B = \{f_i; i \in \mathbb{N}\}$  é uma base. Claramente  $B$  é um conjunto linearmente independente, mostremos que ele gera  $R$ .

Seja  $f \in R$  temos que existe um  $f_k \in B$  tal que  $\rho(f_k) = \rho(f)$  o que nos dá que existe  $\lambda_k \in \mathbb{F}$  de modo que,  $\rho(f - \lambda_k f_k) < \rho(f_k)$ , novamente temos que existe  $f_h$  com  $h < k$  tal que  $\rho(f - \lambda_k f_k) = \rho(f_h)$  e conseqüentemente existe  $\lambda_h$  tal que  $\rho(f - \lambda_k f_k - \lambda_h f_h) < \rho(f_h)$ , esse processo deve acabar em no máximo  $k$  vezes pois temos apenas  $k - 1$   $\rho_i$ 's menores que  $\rho_k$ . Assim chegaremos em  $\rho(f - \sum_{i=0}^{k-1} \lambda_{k-i} f_{k-i}) < \rho(1)$ , observe que alguns dos  $\lambda_i$ 's que aparecem aqui podem ser nulos,  $\rho(f - \sum_{i=0}^{k-1} \lambda_{k-i} f_{k-i}) = -\infty$  o que nos dá que  $f = \sum_{i=0}^{k-1} \lambda_{k-i} f_{k-i}$ , assim  $B$  é uma  $\mathbb{F}$ -base de  $R$ .

(2) Pela existência da base acima e o fato de que  $\rho(f + g) = \max\{\rho(f), \rho(g)\}$  se  $\rho(f) \neq \rho(g)$ , tem-se (2).

(3) Como  $\rho(f_i) < \rho(f_{i+1})$  temos que  $\rho(f_i f_j) < \rho(f_{i+1} f_j)$  logo  $l(i, j) < l(i+1, j)$ .

(4) Sendo  $\rho$  uma função peso temos que  $\rho(fg) = \rho(f) + \rho(g)$ . Assim  $\rho_{l(i,j)} = \rho_i + \rho_j$ . □

## 3.2 Códigos de Avaliação

Nessa seção introduziremos o conceito de código de avaliação. Trabalharemos aqui com um corpo finito com  $q$  elementos,  $\mathbb{F}_q$ . Além disso, aqui  $R$  é uma  $\mathbb{F}_q$ -álgebra com função ordem  $\rho$  tal que admite uma base,  $\{f_i; i \in \mathbb{N}\}$ , de modo que  $\rho(f_i) < \rho(f_{i+1})$  para todo  $i \in \mathbb{N}$ .

Queremos transformar o espaço vetorial  $\mathbb{F}_q^n$  em uma álgebra e para isso precisamos definir uma multiplicação de vetores, assim definiremos a multiplicação  $*$  como sendo a multiplicação usual de coordenadas, ou seja, dados  $a = (a_1, \dots, a_n), b = (b_1, \dots, b_n) \in \mathbb{F}_q^n$  temos que  $a * b = (a_1 b_1, \dots, a_n b_n)$ .

**Definição 3.2.1.** Definimos por  $L_l$  o espaço vetorial gerado por  $f_1, \dots, f_l$ .

**Definição 3.2.2.** Chamaremos de **morfismo de  $\mathbb{F}_q$ -álgebras**, a uma função  $\mathbb{F}_q$ -linear,  $\varphi : R \rightarrow \mathbb{F}_q^n$ , tal que  $\varphi(fg) = \varphi(f) * \varphi(g)$ .

Agora definiremos um código de avaliação e o seu código dual.

**Definição 3.2.3.** Seja  $L_l$  o espaço vetorial como acima definido e  $\varphi$  um morfismo entre  $\mathbb{F}_q$ -álgebras, assim definimos o **código de avaliação  $E_l$**  determinado por  $\varphi$ , como sendo a imagem de  $L_l$  por meio da função  $\varphi$ , ou seja,

$$E_l = \varphi(L_l) = \langle \varphi(f_1), \dots, \varphi(f_l) \rangle.$$

Denotaremos por  $C_l$  o código dual de  $E_l$ .

Observe que a sequência de códigos  $(E_l)_{l \in \mathbb{N}}$  é crescente segundo a inclusão, e mais, como o espaço de chegada da função  $\varphi$  tem dimensão finita temos que essa sequência estabiliza num certo  $N$ .

Trabalharemos aqui somente com os morfismos sobrejetivos.

**Exemplo 3.2.4.** Sejam  $R = \mathbb{F}_q[x_1, \dots, x_n]/I$ , onde  $I$  é um ideal do anel de polinômios  $\mathbb{F}_q[x_1, \dots, x_n]$ ,  $\mathcal{P} = \{P_1, \dots, P_m\}$  um subconjunto com  $m$  pontos de  $V(I)$ , consideremos a função de avaliação:

$$\begin{aligned} ev_{\mathcal{P}} : R &\rightarrow \mathbb{F}_q^m \\ f + I &\mapsto (f(P_1), \dots, f(P_m)) \end{aligned}.$$

Observe que  $ev_{\mathcal{P}}$  está bem definida, pois para  $P \in V(I)$  temos que se  $f + I = g + I$  então  $f - g \in I$ , logo,  $(f - g)(P) = 0$ , ou seja,  $f(P) = g(P)$ , e mais, desse modo definido  $ev_{\mathcal{P}}$  é um morfismo de  $\mathbb{F}_q$ -álgebras, visto que  $fg(P) = f(P)g(P)$ , para todos  $f, g \in R$  e  $P \in \mathbb{F}_q^n$ .

**Lema 3.2.5.** *A função de avaliação acima definida é sobrejetiva.*

*Demonstração.* Sejam  $P_j = (a_{j1}, \dots, a_{jm})$  e os conjuntos auxiliares  $A_{il} = \{a_{jl}; j = 1, \dots, m\} \setminus \{a_{il}\}$ . Definimos os polinômios

$$G_i = \prod_{l=1}^n \prod_{a \in A_{il}} (x_l - a).$$

Temos que  $G_i(P_j) = 0$  sempre que  $i \neq j$ , e mais  $G_i(P_i) \neq 0$ . Os polinômios  $G_i/G_i(P_i)$  quando aplicados em  $ev_{\mathcal{P}}$  chegam na base canônica de  $\mathbb{F}_q^n$  assim  $ev_{\mathcal{P}}$  é sobrejetiva.  $\square$

### 3.3 A Cota Ordem

Um dos principais parâmetros de uma código é a sua distância mínima, contudo, na maioria das vezes é difícil de ser calculada, assim torna-se importante as cotas para essa distância mínima. Nesta seção estamos interessados em encontrar uma cota inferior para a distância mínima do código  $C_l$ .

Continuaremos a usar as notações da seção anterior, lembrando que  $N$  é o menor natural tal que a sequência de códigos de avaliação  $E_l$  estabiliza. Os morfismos utilizados serão sobrejetivos.

Definimos aqui uma  $N \times n$  matriz  $H$  com a  $i$ -ésima linha sendo  $h_i = \varphi(f_i)$  onde  $f_i$  são os elementos da base construída anteriormente e  $\varphi$  é o morfismo de  $\mathbb{F}_q$ -álgebras utilizado aqui.

**Definição 3.3.1.** *Seja  $y \in \mathbb{F}_q^n$ . Consideremos as síndromes  $s_i(y) = \langle y, h_i \rangle$  e  $s_{ij}(y) = \langle y, (h_i * h_j) \rangle$ . Então a matriz  $S(y) = (s_{ij}(y); 1 \leq i, j \leq N)$  é a matriz síndrome de  $y$ .*

**Lema 3.3.2.** *Seja  $y \in \mathbb{F}_q^n$  e  $D(y)$  a matriz diagonal com as coordenadas de  $y$  em sua diagonal, então*

$$S(y) = HD(y)H^t,$$

e mais

$$\text{posto}(S(y)) = w(y).$$

*Demonstração.* Temos que  $s_{ij}(y) = \langle y, (h_i * h_j) \rangle = \sum_l y_l h_{il} h_{jl}$ , e mais, denotando  $C = S(y)$ , temos que  $C_{ij} = H_{ik} y_k H_{kj}^t = H_{ik} y_k H_{jk}$ , logo a igualdade é válida.

Agora o posto de  $D(y)$  é justamente o peso de  $y$ . Como a função  $\varphi$  é sobrejetiva temos que a matriz  $H$  tem posto máximo, ou seja, posto de  $H$  é  $n$ . Assim temos que o posto de  $S(y)$  é o mesmo posto de  $D(y)$  como queríamos.  $\square$

**Definição 3.3.3.** *Seja  $l \in \mathbb{N}_0$ , definimos o conjunto  $N_l = \{(i, j) \in \mathbb{N}^2; l(i, j) = l + 1\}$ , onde  $l(i, j)$  é o número natural definido no item 3 do teorema 3.1.8. A sua cardinalidade denotaremos por  $\nu_l$ .*

**Lema 3.3.4.** *Se  $t = \nu_l$  e  $(i_1, j_1), \dots, (i_t, j_t)$  é a enumeração dos elementos de  $N_l$  em ordem crescente segundo a ordem lexicográfica<sup>1</sup> em  $\mathbb{N}^2$ . Então  $i_1 < i_2 < \dots < i_t$  e  $j_t < j_{t-1} < \dots < j_1$ . Além disso, se  $y \in C_l \setminus C_{l+1}$  temos que  $s_{i_u j_v}(y) = 0$  se  $u < v$  e  $s_{i_u j_v}(y) \neq 0$  se  $u = v$ .*

*Demonstração.* Pela ordem da seqüência temos que  $i_1 \leq i_2 \leq \dots \leq i_t$ , suponha por absurdo que  $i_k = i_{k+1}$ . Desse modo temos que  $j_k < j_{k+1}$  logo

$$l + 1 = l(i_k, j_k) < l(i_k, j_{k+1}) = l(i_{k+1}, j_{k+1}) = l + 1$$

absurdo, logo a seqüência é estritamente crescente.

Agora suponha que  $j_k \geq j_{k+1}$ , novamente temos que

$$l + 1 = l(i_k, j_k) \geq l(i_k, j_{k-1}) > l(i_{k-1}, j_{k-1}) = l + 1,$$

outro absurdo, assim essa seqüência é decrescente.

Seja  $y \in C_l$ , se  $u < v$  temos que  $l(i_u, j_v) < l(i_v, j_v) = l + 1$ , assim  $f_{i_u} f_{j_v} \in L_l$  e desse modo  $h_{i_u} * h_{j_v} \in E_l$ , logo  $s_{i_u j_v}(y) = \langle y, h_{i_u} * h_{j_v} \rangle = 0$ . Do mesmo modo se

---

<sup>1</sup>Dados  $(a, b), (c, d) \in \mathbb{N}^2$ ,  $(a, b) < (c, d)$  se  $a < c$  ou  $a = c$  e  $b < d$ .

$u = v$  temos que  $l(i_u, j_v) = l + 1$  o que nos dá que  $h_{i_u} * h_{j_v} \in L_{l+1} \setminus L_l$ , e mais,  $f_{i_u} f_{j_v} \equiv \mu f_{l+1} \pmod{L_l}$  para algum  $0 \neq \mu \in \mathbb{F}_q$ . Assim  $h_{i_u} * h_{j_v} \equiv \mu h_{l+1} \pmod{E_l}$ , como  $y \notin C_l$  temos que  $s_{l+1}(y) = \langle y, h_{l+1} \rangle \neq 0$  pois  $\langle h_i, y \rangle = 0$  para  $1 \leq i \leq l$  e  $h_{l+1} \notin C_l$ . Assim  $s_{i_u j_v}(y) \neq 0$ .  $\square$

Observamos que a matriz  $m_{uv} = s_{i_u j_v}(y)$  com  $1 \leq u, v \leq \nu_l$  como do lema acima, é uma matriz quadrada de posto  $\nu_l$ , e mais,  $(m_{uv})$  é uma sub-matriz de  $S(y)$ , logo o posto de  $S(y)$  é maior ou igual a  $\nu_l$ . Isso juntamente como os lemas 3.3.2 e 3.3.4 demonstram a seguinte proposição:

**Proposição 3.3.5.** *Se  $y \in C_l \setminus C_{l+1}$ , então  $w(y) \geq \nu_l$ .*

Definiremos agora algumas cotas relacionadas aos códigos de avaliação.

**Definição 3.3.6.** *Chamaremos de cota ordem aos números*

$$d(l) = \min\{\nu_m; m \geq l\},$$

$$d_\varphi(l) = \min\{\nu_m; m \geq l, C_m \neq C_{m+1}\}.$$

**Teorema 3.3.7.** *Os números  $d(l)$  e  $d_\varphi(l)$  são cotas inferiores para a distância mínima de  $C_l$ . Mais ainda,  $d(C_l) \geq d_\varphi(l) \geq d(l)$ .*

*Demonstração.* Pela proposição 3.3.5 temos que  $d(C_l) \geq \nu_l \geq d_\varphi(l)$ .  $\square$

## 3.4 Semigrupos

Nesta seção falaremos de semigrupos e a sua associação aos códigos de avaliação.

**Definição 3.4.1.** *Um semigrupo numérico é um subconjunto  $\Lambda$  de  $\mathbb{N}_0$  com as seguintes propriedades:*

1.  $\Lambda$  é fechado para adição;
2.  $0 \in \Lambda$ .

*Os elementos de  $\mathbb{N}_0 \setminus \Lambda$  são chamados de lacunas e a quantidade desses elementos será denotada por  $g = g(\Lambda)$  (aqui  $g$  pode ser infinito).*

Suponha agora  $\rho$  é uma função peso em uma  $\mathbb{F}_q$ -álgebra  $R$ , por 3.1.2-6 temos que o conjunto  $\Lambda = \{\rho(f); f \in R, f \neq 0\}$  é um semigrupo numérico chamado de **semigrupo de  $\rho$** . Se  $g < \infty$ , então existe um  $n \in \Lambda$  tal que se  $x \in \mathbb{N}$  e  $n \leq x$  então  $x \in \Lambda$ . Ao menor  $n$  com essa propriedade chamamos de *condutor* de  $\Lambda$  e denotamos por  $c = c(\Lambda)$ . Observe que  $c - 1$  é o maior lacuna de  $\Lambda$  desde que  $g > 0$ .

**Definição 3.4.2.** *Seja  $(\rho_l)_{l \in \mathbb{N}}$  uma enumeração do semigrupo  $\Lambda$  tal que  $\rho_l < \rho_{l+1}$  para todo  $l$ . Denotamos por  $g(l)$  o número de lacunas menores que  $\rho_l$ .*

**Lema 3.4.3.** *Sejam  $\Lambda$  um semigrupo com finitos lacunas e  $l \in \mathbb{N}$ , então:*

1.  $g(l) = \rho_l - l + 1$ ;
2.  $\rho_l \leq l + g - 1$ , valendo a igualdade se, e somente se,  $\rho_l \geq c$ ;
3. Se  $l > c - g$ , então  $\rho_l = l + g - 1$ ;
4. Se  $l \leq c - g$ , então  $\rho_l < c - 1$ .

*Demonstração.* (1) O elemento  $\rho_l \in \Lambda$  é o  $(\rho_l + 1)$ -ésimo elemento de  $\mathbb{N}_0$  e mais, ele é o  $(\rho_l + 1 - g(l))$ -ésimo elemento de  $\Lambda$ . Assim  $l = \rho_l + 1 - g(l)$ , ou seja,  $g(l) = \rho_l + 1 - l$ .

(2) Se  $g(l) \leq g$  temos que  $\rho_l + 1 - l \leq g$ , logo  $\rho_l \leq g - 1 + l$ , se  $\rho_l \geq c$  temos que todos os lacunas são menores que  $\rho_l$  logo  $g(l) = g$  valendo assim a igualdade.

(3) Temos que  $c$  é o  $(c+1)$ -ésimo elemento de  $\mathbb{N}_0$  e mais, é o  $(c+1-g)$ -ésimo termo de  $\Lambda$ , assim  $c = \rho_{c+1-g}$ . Tomando  $l > c - g$  teremos  $\rho_l \geq \rho_{c+1-g} = c$  e mais, conseguimos assim  $\rho_l = g - 1 + l$ .

(4) Seja  $l \leq c - g$ , assim  $\rho_l \leq l + g - 1 \leq c - 1$ . Contudo  $c - 1$  é um lacuna ou é negativo. Para  $c = 0$  não tem sentido a proposição, então temos que  $c - 1$  é um lacuna, assim  $\rho_l < c - 1$ .  $\square$

A próxima proposição nos traz um resultado sobre o condutor de um semigrupo numérico que vai influenciar em uma importante definição.

**Proposição 3.4.4.** *Seja  $\Lambda$  um semigrupo numérico com número de lacunas  $g < \infty$ , então  $c \leq 2g$  e a igualdade é válida se, e somente se, para todo lacuna  $s$  temos que  $c - 1 - s$  não é um lacuna.*



*Demonstração.* Observemos que os pares  $(s, t) \in \mathbb{N}_0^2$  tais que  $s + t = c - 1$ , pelo fato de  $c - 1$  ser um lacuna e de  $\Lambda$  ser fechado em relação a soma, tem pelo menos um dos dois termos de cada par como um lacuna. Como temos  $c$  pares desses, levando em consideração a ordem, temos que existem pelo menos  $\left\lfloor \frac{c+1}{2} \right\rfloor$  lacunas, logo  $c \leq 2g$ .

Agora se a igualdade é válida, temos que  $g = \frac{c}{2}$  assim dados  $s, t \in \mathbb{N}_0$  tais que  $s + t = c - 1$  temos que apenas um dos dois ( $s$  ou  $t$ ) é um lacuna, logo sendo  $s$  um lacuna  $c - 1 - s$  não pode ser lacuna.

Supondo que se  $s$  for um lacuna temos que  $c - 1 - s$  não é, isso nos dá que apenas um dos termos dos pares  $(s, t)$  tais que  $s + t = c - 1$  é um lacuna, assim temos exatamente  $\frac{c}{2}$  lacunas.  $\square$

O resultado anterior justifica a seguinte definição:

**Definição 3.4.5.** *Um semigrupo numérico é chamado simétrico se  $c = 2g$ .*

**Definição 3.4.6.** *Dizemos que um semigrupo numérico é finitamente gerado se existe um conjunto  $A = \{a_1, \dots, a_k\} \subset \Lambda$  tal que dado  $\lambda \in \Lambda$  temos que existem  $x_1, \dots, x_k \in \mathbb{N}_0$ , tais que  $\lambda = \sum_{i=1}^k x_i a_i$ . Assim falamos que  $A$  gera  $\Lambda$  e escrevemos  $\Lambda = \langle A \rangle$ .*

A respeito de subgrupos numéricos finitamente gerados o primeiro resultado que apresentamos é:

**Proposição 3.4.7.** *Sejam  $a, b \in \mathbb{N}$  tais que  $\text{mdc}(a, b) = 1$ . O semigrupo gerado por  $a$  e  $b$  é simétrico, tem como último lacuna o número  $ab - a - b$ , como seu condutor o número  $(a - 1)(b - 1)$  e o número total de lacunas é  $(a - 1)(b - 1)/2$ .*

*Demonstração.* Como  $\text{mdc}(a, b) = 1$ , temos que todo inteiro  $m$  pode ser escrito como  $m = xa + yb$ , de maneira única com  $0 \leq y < b$ .

Pelo fato acima observamos que o maior lacuna possível é  $(b - 1)a - b$  e de fato esse número é um lacuna, pois não é possível escreve-lo como  $(b - 1)a - b = xa + yb$  com  $x, y \in \mathbb{N}_0$ , assim temos que o condutor é  $c = (b - 1)a - b + 1 = (a - 1)(b - 1)$ .

Agora mostremos que o semigrupo é simétrico. Suponhamos por absurdo que o semigrupo não seja simétrico, ou seja, existe  $s, t \in \mathbb{N}$  lacunas tais que  $s + t = c - 1$

onde  $c$  é o condutor. Podemos escrever  $s = x_1a + y_1b$  e  $t = x_2a + y_2b$ , assim temos que  $c - 1 = ab - a - b = (x_1 + x_2)a + (y_1 + y_2)b$ . Observe que  $0 \leq x_1 + x_2 \leq 2b - 2$  e mais  $y_1 + y_2 \leq -2$ . Disto segue que:

$$D = (-y_1 - y_2 - 1)b = (x_1 + x_2 - b + 1)a \Rightarrow$$

$$0 < b \leq (-y_1 - y_2 - 1)b = (x_1 + x_2 - b + 1)a \leq (b - 1)a < ba$$

Como  $\text{mdc}(a, b) = 1$  temos que  $a | (-y_1 - y_2 - 1)$  e que  $b | (x_1 + x_2 - b + 1)$ , assim chegamos que  $0 < \frac{D}{ab} < 1$ , absurdo, logo  $\Lambda$  é simétrico.

Como o semigrupo é simétrico temos que  $c = 2g$ , logo  $g = (a - 1)(b - 1)/2$ .  $\square$

Faremos agora mais um lema técnico sobre semigrupos.

**Lema 3.4.8.** *Sejam  $\Lambda$  um semigrupo numérico com finitos lacunas e  $s \in \Lambda$ . Então temos que  $\#(\Lambda \setminus \{s + \lambda; \lambda \in \Lambda\}) = s$ .*

*Demonstração.* Seja  $c$  o condutor de  $\Lambda$ ,  $T = \{t \in \mathbb{N}_0; t \geq s + c\}$ , claramente temos que  $T \subset \Lambda$ , e mais,  $T \subset s + \Lambda = \{s + \lambda; \lambda \in \Lambda\}$ . Seja  $U = \{u \in \Lambda; u < s + c\}$ , temos que  $\#U = s + c - g$ , além disso  $\Lambda = U \cup T$ . Seja  $V = \{v \in s + \Lambda; s \leq v < s + c\}$ , temos que  $\#V = s + c - g - s = c - g$ , e mais,  $s + \Lambda = V \cup T$ . Observe que as uniões acima são disjuntas e mais,  $V \subset U$ . Assim temos que:

$$\#(\Lambda \setminus s + \Lambda) = \#(U \cup T \setminus V \cup T) = \#(U \setminus T) = s + c - g - (c - g) = s.$$

Como queríamos demonstrar.  $\square$

Uma consequência quase imediata desse lema é:

**Proposição 3.4.9.** *Seja  $f$  um elemento não nulo de uma  $\mathbb{F}_q$ -álgebra  $R$  com uma função peso  $\rho$ . Então  $\dim_{\mathbb{F}_q}(R/\langle f \rangle) = \rho(f)$ .*

*Demonstração.* Sejam  $\Lambda$  o semigrupo da função peso  $\rho$  e  $s = \rho(f)$ . Tomemos a sequência  $(\rho_i)_{i \in \mathbb{N}}$  dos elementos de  $\Lambda$  em ordem crescente. Pela propriedade 3.1.2-6 temos que a imagem dos elementos não nulos do ideal  $\langle f \rangle$  segundo a função  $\rho$  é o conjunto  $s + \Lambda$ . Como feito antes, para todo  $\rho_i \in \Lambda$ , existe um  $f_i \in R$  tal que  $\rho(f_i) = \rho_i$  e caso  $\rho_i \in s + \Lambda$  podemos tomar  $f_i \in \langle f \rangle$ . Os conjuntos  $\{f_i; i \in \mathbb{N}\}$  e  $\{f_i; i \in \mathbb{N}, \rho_i \in s + \Lambda\}$  formam uma base para a álgebra  $R$  e o

ideal  $\langle f \rangle$  respectivamente, vide demonstração de 3.1.8. Desse modo as classes de equivalência  $f_i$  módulo  $\langle f \rangle$  com  $i \in \mathbb{N}$  e  $\rho_i \in \Lambda \setminus (s + \Lambda)$  formam uma base para o quociente  $R/\langle f \rangle$ . Assim a sua dimensão é a cardinalidade da base que é  $s$  pelo lema 3.4.8, ou seja,  $\rho(f)$ .  $\square$

**Definição 3.4.10.** *Seja  $R = \mathbb{F}_q[x_1, \dots, x_n]/I$ , onde  $I$  é um ideal do anel de polinômios  $\mathbb{F}_q[x_1, \dots, x_n]$ , para  $f + I \in R$  dizemos que  $P \in \mathbb{F}_q^n$  é um zero de  $f + I$ , se  $P \in V(I)$  e  $f(P) = 0$ .*

**Lema 3.4.11.** *Seja  $R$  uma  $\mathbb{F}_q$ -álgebra finita com uma função peso  $\rho$ . Seja  $f \in R$  um elemento não nulo. Então o número de zeros de  $f$  é no máximo  $\rho(f)$ .*

*Demonstração.* Seja  $\mathcal{P}$  o conjunto de zeros de  $f$  e  $t = \#\mathcal{P}$ . A função de avaliação,  $ev_{\mathcal{P}} : R \rightarrow \mathbb{F}_q^t$ , é uma função linear e pelo lema 3.2.5 temos que  $ev_{\mathcal{P}}$  é sobrejetiva. Isso nos garante que  $R/\text{Ker}(ev_{\mathcal{P}}) \simeq \mathbb{F}_q^t$ . Observe que  $\langle f \rangle \subset \text{Ker}(ev_{\mathcal{P}})$  e olhando ambos como sub-espço vetorial de  $R$  temos que  $\dim_{\mathbb{F}_q}(\langle f \rangle) \leq \dim_{\mathbb{F}_q}(\text{Ker}(ev_{\mathcal{P}}))$ . Assim segue que  $t = \dim_{\mathbb{F}_q}(R/\text{Ker}(ev_{\mathcal{P}})) = \dim_{\mathbb{F}_q}(R) - \dim_{\mathbb{F}_q}(\text{Ker}(ev_{\mathcal{P}})) \leq \dim_{\mathbb{F}_q}(R) - \dim_{\mathbb{F}_q}(\langle f \rangle) = \dim_{\mathbb{F}_q}(R/\langle f \rangle) = \rho(f)$  por 3.4.9.  $\square$

## 3.5 Código de Avaliação Via Semigrupos

Aqui estamos interessados em encontrar uma cota para a distância mínima dos códigos de avaliação  $E_l$ .

Nessa seção iremos supor que  $\rho$  é uma função peso em  $R = \mathbb{F}_q[x_1, \dots, x_m]/I$ , onde  $I$  é um ideal de  $\mathbb{F}_q[x_1, \dots, x_m]$  (anel de polinômios em  $m$  variáveis). Seja  $(\rho_i)_{i \in \mathbb{N}}$  a enumeração do semigrupo de  $\rho$  em ordem crescente. Tomemos  $\mathcal{P}$  como um conjunto com  $n$  pontos do conjunto  $V(I)$  (variedade algébrica gerada por  $I$ ). A função de avaliação  $ev_{\mathcal{P}} : R \rightarrow \mathbb{F}_q^n$  nos define os códigos de avaliação

$$E_l = \{ev_{\mathcal{P}}(f); f \in R, \rho(f) \leq \rho_l\}.$$

**Teorema 3.5.1.** *A distância mínima do código  $E_l$  é maior ou igual a  $n - \rho_l$ . Se  $\rho_l < n$ , temos que  $\dim_{\mathbb{F}_q}(E_l) = l$ .*

*Demonstração.* Seja  $c$  uma palavra código não nula de  $E_l$ , então existe  $f \in R \setminus \{0\}$  tal que  $\rho(f) \leq \rho_i$  e  $c = ev_{\mathcal{P}}(f)$ . Temos que  $c_i = f(P_i)$  para todo  $0 < i < n + 1$ , onde os  $c_i$ 's são as coordenadas da palavra  $c$ , pelo lema 3.4.11 temos que o número de zeros de  $f$  é no máximo  $\rho(f) \leq \rho_l$ , assim  $w(c) \geq n - \rho_l$ .

Agora suponha que  $\rho_l < n$ . Temos que  $E_l$  é a imagem do espaço vetorial  $L_l$  através da função  $ev_{\mathcal{P}}$ . Se  $f \in L_l$  e  $ev_{\mathcal{P}}(f) = 0$  então  $f$  tem pelo menos  $n$  zeros, mas pelo lema 3.4.11 se  $f$  é não nulo então  $f$  admite no máximo  $\rho(f)$  zeros, contudo  $\rho(f) \leq \rho_l < n$ , assim  $f$  tem de ser nulo, concluimos assim que  $Ker(ev_{\mathcal{P}}|_{L_l}) = \{0\}$ , o que nos dá que  $\dim_{\mathbb{F}_q}(E_l) = \dim_{\mathbb{F}_q}(L_l)$ , lembremos que  $L_l$  é o espaço vetorial gerado pelo conjunto  $\{f_1, \dots, f_l\}$ , logo sua dimensão é  $l$ , assim  $\dim_{\mathbb{F}_q}(E_l) = l$ .  $\square$

**Corolário 3.5.2.** *Seja  $\rho$  uma função peso com  $g$  lacunas. Se  $\rho_k < n$ , então  $E_k$  é um  $[n, k, d]$ -código tal que  $d \geq n + 1 - k - g$ .*

*Demonstração.* Pelo teorema 3.5.1 temos que  $d \geq n - \rho_k$ . Agora pelo lema 3.4.3 temos que  $\rho_k \leq k + g - 1$ , assim segue que  $d \geq n + 1 - k - g$ .  $\square$

# Capítulo 4

## Exemplos

Este capítulo está dedicado a apresentação de alguns exemplos dos códigos que nesse texto foram definidos. As notações aqui utilizadas são na maioria as mesmas do capítulo 3, ou seja,  $R$  denotará sempre uma  $\mathbb{F}_q$ -álgebra,  $\rho$  uma função peso,  $l(i, j)$ , o inteiro tal que  $\rho(f_i f_j) = \rho_{l(i, j)}$ , onde  $\{f_1, f_2, \dots\}$  é uma  $\mathbb{F}_q$ -base para  $R$ , etc.

### 4.1 Um Primeiro Exemplo

Esse primeiro teorema do capítulo vai nos permitir garantir a existência de funções ordem e peso em determinadas condições.

**Teorema 4.1.1.** *Sejam  $R$  uma  $\mathbb{F}$ -álgebra e  $\{f_1, f_2, \dots\}$  uma  $\mathbb{F}$ -base do  $\mathbb{F}$ -espaço vetorial  $R$ , com  $f_1 = 1$ . Sejam, ainda,  $(\rho_i)_{i \in \mathbb{N}}$  uma seqüência estritamente crescente de inteiros não negativos e  $\rho : R \rightarrow \mathbb{N}_0 \cup \{-\infty\}$  a função definida por  $\rho(0) = -\infty$  e  $\rho(f) = \rho_i$  se  $f \neq 0$  e  $i$  for o menor inteiro tal que  $f \in L_i$ , onde  $L_i$  é o  $\mathbb{F}$ -subespaço vetorial gerado por  $\{f_1, \dots, f_i\}$ . Se para todo  $(i, j) \in \mathbb{N}^2$  tem-se que  $l(i, j) < l(i + 1, j)$ , então  $\rho$  é uma função ordem e, mais ainda, se  $\rho_{l(i, j)} = \rho_i + \rho_j$ , então  $\rho$  é uma função peso.*

*Demonstração.* Diretamente da definição da função  $\rho$ , vemos que ela satisfaz as condições 1, 2, 3 e 5 para ser uma função peso. Mostraremos que ela também satisfaz as outras duas condições (4 e 6).

Para  $f \in R \setminus \{0\}$ , associamos o número  $\iota(f)$ , o qual é o menor inteiro positivo tal que  $f \in L_{\iota(f)}$ . Dados  $f, g \in R \setminus \{0\}$  temos que

$$f = \sum_{i \leq \iota(f)} \lambda_i f_i, g = \sum_{i \leq \iota(g)} \nu_i f_i f g = \sum_{i \leq \iota(fg)} \mu_i f_i \text{ e } f_i f_j = \sum_{l \leq l(i,j)} \eta_{ijl} f_l.$$

com  $\lambda_{\iota(f)} \neq 0$ ,  $\nu_{\iota(g)} \neq 0$ ,  $\mu_{\iota(fg)} \neq 0$  e  $\eta_{ijl(i,j)} \neq 0$ .

Observe que

$$\begin{aligned} fg &= \left( \sum_{i \leq \iota(f)} \lambda_i f_i \right) \left( \sum_{j \leq \iota(g)} \nu_j f_j \right) = \sum_{i \leq \iota(f)} \sum_{j \leq \iota(g)} \lambda_i \nu_j f_i f_j = \\ &= \sum_{i \leq \iota(f)} \sum_{j \leq \iota(g)} \lambda_i \nu_j \sum_{l \leq l(i,j)} \eta_{ijl} f_l = \sum_{i \leq \iota(f)} \sum_{j \leq \iota(g)} \sum_{l \leq l(i,j)} \lambda_i \nu_j \eta_{ijl} f_l, \end{aligned}$$

assim temos que

$$\mu_l = \sum_{l(i,j)=l} \lambda_i \nu_j \eta_{ijl} f_l.$$

Por hipótese temos que  $l(i, j) < l(i+1, j)$ , assim  $l(i, j) < l(\iota(f), \iota(g))$  se  $i < \iota(f)$  ou  $j < \iota(g)$ . Supondo  $i = \iota(f)$  e  $j = \iota(g)$ , temos que  $\mu_{fg} = \lambda_i \nu_j \eta_{ijl(i,j)} \neq 0$ , o que nos garante que  $\iota(fg) = l(\iota(f), \iota(g))$ .

Agora dados  $f, g, h \in R \setminus \{0\}$ , com  $\rho(f) < \rho(g)$ , temos que  $\rho(fh) = \rho_{\iota(fh)} = \rho_{l(\iota(f), \iota(h))} < \rho_{l(\iota(g), \iota(h))} = \rho_{\iota(gh)} = \rho(gh)$ , logo a condição 4 é verificada e  $\rho$  é uma função ordem.

Agora assumindo que  $\rho_{l(i,j)} = \rho_i + \rho_j$ , temos que  $\rho(fg) = \rho_{\iota(fg)} = \rho_{l(\iota(f), \iota(g))} = \rho_{\iota(f)} + \rho_{\iota(g)} = \rho(f) + \rho(g)$ . Ou seja, a condição 6 também é satisfeita sendo então  $\rho$  uma função peso.  $\square$

**Exemplo 4.1.2.** Seja  $\mathcal{X}$  a curva definida pelo polinômio  $P(x, y) \in \mathbb{F}_q[x, y]$ ,  $P(x, y) = x^m + y^{m-1} + G(x, y)$ , com  $gr_{\text{total}}(G(x, y)) < m - 1$ . Como  $P(x, y)$  é um polinômio irredutível, temos que o anel  $R = \mathbb{F}_q[x, y]/\langle P(x, y) \rangle$  é um domínio de integridade e mais,  $R$  é uma  $\mathbb{F}_q$ -álgebra. Assim, construído  $R$  e denotando por  $\bar{x}, \bar{y}$  as classes de equivalências  $x + \langle P(x, y) \rangle$  e  $y + \langle P(x, y) \rangle$ , respectivamente, temos que  $R$  admite uma função peso,  $\rho$ , tal que  $\rho(\bar{x}) = m - 1$  e  $\rho(\bar{y}) = m$ .

*Demonstração.* O conjunto  $B = \{\bar{x}^\alpha \bar{y}^\beta \in R; \alpha < m\}$ , é uma  $\mathbb{F}_q$ -base para  $R$ . De fato, primeiro observemos que  $\bar{x}^m = -\bar{y}^{m-1} - \bar{G}$ , e dado  $\bar{h} \in R$  temos

que  $\bar{h} = h(x, y) + \langle P(x, y) \rangle$  e mais,  $h(x, y) = \sum_{i=0}^a \sum_{j=0}^b \lambda_{ij} x^i y^j$ , com  $\lambda_{ab} \neq 0$ . Para demonstrar que  $B$  gera  $R$  vamos supor sem perda de generalidade que  $h(x, y)$  é um monômio, visto que no máximo ele é uma soma de monômios, assim  $h(x, y) = x^a y^b$ , se  $a < m$  temos que  $h(x, y) \in B$  assim não temos o que fazer, suponha então  $a \geq m$ .

Podemos escrever  $a = km + c$  com  $c < a$ , assim  $\bar{x}^a \bar{y}^b = \bar{x}^c \bar{y}^b (-\bar{y}^{m-1} - \bar{g})^k$ , temos que  $\bar{x}^c \bar{y}^{b+k(m-1)} \in B$  e os demais monômios de  $\bar{x}^c \bar{y}^b (-\bar{y}^{m-1} - \bar{g})^k$  tem grau em  $x$  menor que  $a$ , logo repetindo esse processo recursivamente para os demais temos que  $\bar{h}$  é escrito como combinação linear de elementos de  $B$ .

Agora queremos mostrar que  $B$  é um conjunto linearmente independente. Seja  $\sum \lambda_{ij} \bar{x}^i \bar{y}^j = 0$  uma soma finita de elementos de  $B$ , equivalentemente mostraremos para  $\sum \lambda_{ij} x^i y^j = f(x, y)P(x, y)$  para algum  $f(x, y) \in \mathbb{F}_q[x, y]$ , temos que se  $f(x, y) \neq 0$ ,  $gr_x(f(x, y)P(x, y)) > m$  e mais,  $gr_x(\sum \lambda_{ij} x^i y^j) < m$  logo a igualdade não é válida, sendo  $f(x, y) = 0$  temos que os  $\lambda'_{ij}$ s são nulos, pois esses monômios são linearmente independentes em  $\mathbb{F}_q[x, y]$  assim  $B$  é uma  $\mathbb{F}_q$ -base para  $R$ .

Seja  $\{f_1, f_2, f_3, \dots\}$  uma enumeração do conjunto  $B$ . Para  $f_i = \bar{x}^\alpha \bar{y}^\beta$  definimos  $\rho_i = \alpha(m-1) + \beta m$ . Sendo  $D = \{(a, b) \in \mathbb{N}_0^2; a < m\}$ , a função  $\varphi : D \rightarrow \mathbb{N}_0$ , tal que  $\varphi(a, b) = a(m-1) + bm$ , é injetiva, já que  $\text{mdc}(m, m-1) = 1$  e  $a < m$ , assim se  $i \neq j$  temos que  $\rho_i \neq \rho_j$ .

Reordenando se preciso, assumiremos que a seqüência  $(\rho_i)_{i \in \mathbb{N}}$  é estritamente crescente.

Seja  $f_i = \bar{x}^\alpha \bar{y}^\beta$  e  $f_j = \bar{x}^\gamma \bar{y}^\delta$ , com  $\alpha < m$  e  $\gamma < m$ . Seguindo as notações do teorema anterior, queremos mostrar que  $l(i, j) < l(i+1, j)$  e para isso vamos mostrar que  $\rho_{l(i, j)} = \rho_i + \rho_j$ . Separaremos em 2 casos,  $\alpha + \gamma < m$  e  $m \leq \alpha + \gamma < 2m$ .

1. Se  $\alpha + \gamma < m$ , temos que  $f_i f_j \in B$ , logo  $f_i f_j = f_{l(i, j)}$ , onde  $l(i, j)$  é o menor inteiro  $l$ , tal que  $f_i f_j \in L_l = \langle f_1, \dots, f_l \rangle$ , assim  $\rho_l(i, j) = \rho_i + \rho_j$ .
2. Agora vamos supor  $\alpha + \gamma \geq m$ , assim  $\alpha + \gamma = m + \epsilon$  com  $0 \leq \epsilon < m$ . Tomamos  $n = \beta + \delta$ , temos que

$$\begin{aligned} f_i f_j &= (\bar{x}^\alpha \bar{y}^\beta)(\bar{x}^\gamma \bar{y}^\delta) = \bar{x}^{(\alpha+\gamma)} \bar{y}^{(\beta+\delta)} = \bar{x}^\epsilon \bar{y}^n (-\bar{y}^{m-1} - \bar{g}) = \\ &= -\bar{x}^\epsilon \bar{y}^{(n+m-1)} - \bar{x}^\epsilon \bar{y}^n \bar{g}. \end{aligned}$$

Observe que  $\bar{x}^\epsilon \bar{y}^{(n+m-1)} \in B$  e mais, se tomarmos  $f_l = \bar{x}^\epsilon \bar{y}^{(n+m-1)}$  temos que

$$\begin{aligned}\rho_i + \rho_j &= (\alpha + \gamma)(m-1) + (\beta + \delta)m = (m + \epsilon)(m-1) + nm = \\ &= \epsilon(m-1) + (m-1+n)m = \rho_l.\end{aligned}$$

Um monômio de  $G$  com coeficiente não nulo é da forma  $x^\kappa y^\lambda$  com  $\kappa \leq gr_x(G) = d$  e  $\kappa + \lambda < m-1$ .

Se  $(\epsilon, \eta), (\kappa, \lambda) \in \mathbb{N}_0^2$ ,  $\epsilon < m$ ,  $\kappa \leq d$ ,  $\kappa + \lambda < m-1$  e  $\rho_l = \epsilon(m-1) + (m-1+n)m$ , então  $\bar{x}^{\epsilon+\kappa} \bar{y}^{\eta+\lambda} \in L_{l-1}$ . De fato, mostraremos isso nos dois casos que seguem.

- (a) Se  $\epsilon + \kappa < m$ , então  $\bar{x}^{\epsilon+\kappa} \bar{y}^{\eta+\lambda} \in B$  e mais,  $(\eta + \lambda)m + (\epsilon + \kappa)(m-1) < \epsilon(m-1) + (\eta + m-1)m = \rho_l$ , assim,  $\bar{x}^{\epsilon+\kappa} \bar{y}^{\eta+\lambda} \in L_{l-1}$ .
- (b) Agora, se  $\epsilon + \kappa \geq m$ , temos que  $\epsilon + \kappa = m + \epsilon'$  com  $\epsilon' < \epsilon$ , pois  $\kappa \leq d < m$  e  $\epsilon < m$ . Do mesmo modo fazemos  $\eta + \lambda = \eta'$ . Assim

$$\bar{x}^{\epsilon+\kappa} \bar{y}^{\eta+\lambda} = \bar{x}^{m+\epsilon'} \bar{y}^{\eta'} = -\bar{x}^{\epsilon'} \bar{y}^{m-1+\eta'} - \bar{x}^{\epsilon'} \bar{y}^{\eta'} \bar{g}.$$

Observe que  $\rho_{l'} = \epsilon'(m-1) + (m-1+\eta')m = (m+\epsilon')(m-1) + \eta'm = (\epsilon + \kappa)(m-1) + (\eta + \lambda)m < \rho_l$ , assim  $f_l \in L_{l-1}$ , e mais, recursivamente podemos mostrar que  $\bar{x}^{\epsilon'} \bar{y}^{\eta'} \bar{g} \in L_{l-1}$ .

Assim mostramos que se  $f_i f_j \in L_{l(i,j)}$  então  $\rho_{l(i,j)} = \rho_i + \rho_j$ .

Desse modo pelo teorema 4.1.1, temos que  $R$  admite uma função peso e que essa do modo que foi construída é gerada por  $m-1$  e  $m$ .  $\square$

**Exemplo 4.1.3.** Seja  $\mathcal{X}$  a curva definida no exemplo 4.1.2. O semigrupo numérico gerado pela função peso  $\rho$ , do mesmo exemplo, tem  $g = \binom{m-1}{2}$  lacunas. Sejam  $Q$  um conjunto de  $n$  pontos racionais de  $\mathcal{X}$  e  $k$  tal que  $\rho_k = lm$ , com  $(l > m, \text{ e } lm < n)$ . O código de avaliação  $C = E_k$ , determinado por  $ev_Q$ , é um  $[n, k, d]$ -código com,  $d \geq n - lm$  e  $k = lm + 1 - g = lm + 1 - \binom{m-1}{2}$ .

*Demonstração.* Temos que o semigrupo determinado  $\rho$  é gerado por  $m$  e  $m-1$ . Assim, pela proposição 3.4.7, temos que  $g = \binom{m-1}{2}$ . Pelo teorema 3.5.1, temos



que  $d \geq n - lm$ . Agora, do lema 3.4.3(1) segue que  $\rho_k = k + g - 1$ , assim  $k = lm - g + 1$ .  $\square$

Note que a dimensão e a cota inferior para a distância mínima do código do último exemplo e do código do teorema 2.2.4 são iguais.

Em vários artigos encontramos referências aos códigos geométricos de Goppa pontuais, códigos da forma  $C(D, mQ)$ , onde  $Q$  é um ponto racional e  $m$  um inteiro. Os códigos de avaliação que aqui construímos foram propostos como um modo de estudo dos códigos de Goppa pontuais de modo simples. A princípio pensava-se que os códigos de avaliação generalisavam os de Goppa pontuais, mas recentemente fora provado que isso é falso. Nos exemplos que seguem fazemos uma associação dos códigos geométricos de Goppa pontuais aos de avaliação.

No livro Algebraic Function Fields and Codes de Hennin Stichtenoth, página 113, temos um exemplo de um corpo de funções no qual o gênero é dado por,  $g = (m - 1)/2$  caso  $m$  seja ímpar e  $g = (m - 2)/2$  caso contrário.

**Exemplo 4.1.4.** Sejam  $K$  um corpo finito de característica diferente de 2,  $\mathcal{X}$  a curva definida por  $y^2 = f(x) = p_1(x) \cdots p_s(x) \in K[x]$ , onde  $p_1(x), \dots, p_s(x)$  são polinômios mônicos irreduzíveis distintos entre si,  $s \geq 1$  e  $F$  o corpo de frações do anel de coordenada de  $\mathcal{X}$ . Assim  $K$  é o corpo de constantes de  $F$  e se  $m = \text{gr}(f(x))$  for ímpar temos que o gênero de  $F$  é  $(m - 1)/2$ .

Agora sejam  $P, P_1, \dots, P_n$ , places de grau 1 dois a dois disjuntos,  $D = P_1 + \cdots + P_n$ ,  $G = lmP$  um divisor em  $F/K$ ,  $m < \text{gr}(G) = lm < n$  e  $\text{supp}(G) \cap \text{supp}(D) = \emptyset$ . Então o código geométrico de Goppa  $C(D, G)$  (definição 2.1.3) tem parâmetros,  $k = lm + 1 - (m - 1)/2$  e  $d \geq n - lm$ .

Faremos agora a construção de um código de avaliação.

**Exemplo 4.1.5.** Sejam  $K$  um corpo finito com característica diferente de 2,  $f(x, y) = y^2 + g(x)$  um polinômio em  $K[x, y]$  tal que  $g(x) \in K[x]$ ,  $\mathcal{X}$  a curva plana gerada por  $f(x, y)$  e  $m = \text{gr}(g(x))$  ímpar, em particular  $f(x, y)$  é irreduzível. Faça  $R = K[x, y]/\langle f(x, y) \rangle$ . Assim  $R$  é uma  $K$ -álgebra que admite uma função peso,  $\rho$ , gerada por 2 e  $m$ .

*Demonstração.* Denotaremos por  $\bar{h}$  à classe  $h + \langle f(x, y) \rangle$  de  $R$ . O conjunto  $B = \{\bar{x}^b \bar{y}^a; a < 2\}$  é uma  $K$ -base para  $R$ . De fato, observe que dada uma soma finita da forma  $\sum \lambda_{ab} \bar{x}^b \bar{y}^a = 0$ , teríamos em  $K[x, y]$  a igualdade  $\sum \lambda_{ab} x^b y^a = h(x, y)f(x, y)$ , para algum  $h(x, y) \in K[x, y]$ , contudo  $gr_y(h(x, y)f(x, y)) \geq 2$  enquanto  $gr_y(\sum \lambda_{ab} x^b y^a) < 2$ , assim  $B$  é um conjunto linearmente independente. Mostremos agora que  $B$  gera  $R$ .

É suficiente mostrar que  $B$  gera os elementos da forma  $\bar{y}^c \bar{x}^d$ , pois todos elementos em  $R$  são somas de elementos desse tipo. Se  $c < 2$  temos que  $\bar{y}^c \bar{x}^d \in B$ , ou seja, não tem o que fazer, vamos supor agora que  $c \geq 2$ .

Podemos então escrever  $c = a + 2k$  com  $a < 2$ , assim  $\bar{y}^c \bar{x}^d = \bar{y}^a \bar{x}^d \overline{g(x)}^k$ , pois  $\bar{y}^2 = \overline{g(x)}$ , logo  $B$  é uma  $K$ -base de  $R$ .

Enumeramos  $B$  como  $\{f_1, f_2, \dots\}$ . Agora sendo  $f_i = \bar{y}^a \bar{x}^b \in B$ , definimos  $\rho_i = 2b + am$ , observe que  $2b + am = 2\tilde{b} + \tilde{a}m$ , com  $a, \tilde{a} < 2$  se, e somente,  $a = \tilde{a}$  e  $b = \tilde{b}$ , visto que  $\text{mdc}(2, m) = 1$ , assim reenumerando caso necessário, assumiremos que  $(\rho_i)_{i \in \mathbb{N}}$  é uma seqüência estritamente crescente.

Seja  $l(i, j)$  o menor inteiro tal que  $f_i f_j \in L_{l(i, j)}$ , queremos mostrar que  $l(i + 1, j) > l(i, j)$ , ou seja, temos que mostrar que  $\rho_{l(i, j)} < \rho_{l(i+1, j)}$ , para isso provaremos que  $\rho_{l(i, j)} = \rho_i + \rho_j$ .

Sejam  $f_i = \bar{x}^a \bar{y}^b$  e  $f_j = \bar{x}^c \bar{y}^d$ , com  $b < 2$  e  $d < 2$ . Se  $b + d < 2$  temos que  $f_i f_j \in B$  e logo  $\rho_{l(i, j)} = \rho_i + \rho_j$ . Suponha agora  $b + d \geq 2$ , temos que  $b + d = 2 + \lambda$  com  $\lambda < 2$ , assim  $f_i f_j = \bar{y}^\lambda \bar{x}^{a+c} \overline{g(x)}$ . Note que para  $f_h = \bar{y}^\lambda \bar{x}^{a+c+m}$ , temos que  $\rho_h = 2a + 2c + 2m + \lambda m = 2(a+c) + m(\lambda+2) = 2(a+c) + m(b+d) = \rho_i + \rho_j$ , observe também que outro monômio  $f_t$  de  $\bar{y}^\lambda \bar{x}^{a+c} \overline{g(x)}$  é tal que  $\rho_t < \rho_h$  assim  $l(i, j) = h$ , concluímos então que  $\rho_{l(i, j)} = \rho_i + \rho_j$  e assim  $\rho_{l(i+1, j)} = \rho_{i+1} + \rho_j > \rho_i + \rho_j = \rho_{l(i, j)}$ .

Agora pelo teorema 4.1.1, temos que existe uma função peso em  $R$ .  $\square$

**Exemplo 4.1.6.** Com as hipóteses do exemplo 4.1.5, tome um conjunto  $P$  com  $n$  pontos racionais distintos de  $\mathcal{X}$ . Além disso, seja  $k$  dado por  $\rho_k = lm$ . Temos então que o código  $E_k$  tem parâmetros iguais ao do código  $C(D, G)$  visto em 4.1.4.

# Referências Bibliográficas

- [1] Fulton, W., **Algebraic Curves**. Benjamin, New York, 1969.
- [2] Garcia, Arnaldo e Lequain, Yves, **Elementos de Álgebra**. Associação Instituto Nacional de Matemática Pura e Aplicada. Rio de Janeiro, 2003. (Projeto Euclides)
- [3] Goppa, V. D., **Codes on Algebraic Curves**. Soviet Math. Dokl. vol 24, No.1, pp. 170-172, 1981.
- [4] Hefez, A. e Villela, M. L. T., **Códigos Corretores de Erros**, (Série Computação e Matemática), IMPA. Rio de Janeiro, 2002.
- [5] Lang, Serge, **Algebra**, Third Edition. Addison-Wesley Publishing Company. Massachusetts, 1997.
- [6] MacWilliams, F. J. and Sloane, N. J. A., **The theory of error-correcting codes**. (North-Holland Mathematical Library; 16). North-Holland, Amsterdam, 1977.
- [7] Stichtenoth, Hennin, **Algebraic Function Fields and Codes**. Springer-Verlag, Berlin, 1993.
- [8] van Lint, J. H., **Introduction to Coding Theory**, 3rd rev. and expanded. Springer - Verlag Berlin Heidelberg New York, New York, 1998.
- [9] van Lint, Jacobus H. , Pellikaan, Ruud and Høhold, Tom, **Algebraic geometry codes** In the Handbook of Coding Theory, vol 1, pp. 871-961, Elsevier, Amsterdam, 1998.

- 
- [10] van Lint, Jacobus H. , Pelikaan, Ruud and Høhold, Tom, **An Elementary Approach to Algebraic Geometry Codes**, Congressus Numerantium 135, pp. 25-35, 1998.